Obtained via FOIA by Judicial Watch, Inc.

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Privacy Office, Mail Stop 0655

December 7, 2018

SENT BY ELECTRONIC MAIL TO: bmarshall@judicialwatch.org

William F. Marshall
Senior Investigator
425 Third Street, SW, Suite 800
Washington, DC 20024

Re: 2017-HQFO-00383

Dear Mr. Marshall:

This is an interim response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated January 26, 2017, and received by this office on February 14, 2017. You are seeking any and all records relating to reported cyberattacks against the Georgia Secretary of State's information network involving DHS and/or its employees or contractors, including but not limited to investigative reports, memoranda, correspondence and communications (Date Range for Record Search: From 10/1/2016 To 2/14/2017).

A search of the office of the Chief Information Officer (CIO) for documents responsive to your request produced a total of 22 pages. Of those pages, I have determined that 3 pages of the records are releasable in their entirety, 19 pages are partially releasable, pursuant to FOIA Exemption 6.

FOIA Exemption 6 exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right to privacy. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

You have a right to appeal the above withholding determination. Should you wish to do so, you must send your appeal and a copy of this letter, within 90 days of the date of this letter, to: Privacy Office, Attn: FOIA Appeals, U.S. Department of Homeland Security, 245 Murray Lane, SW, Mail Stop 0655, Washington, D.C. 20528-0655, following the procedures outlined in the DHS FOIA regulations at 6 C.F.R. Part 5 § 5.8. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS FOIA regulations are available at www.dhs.gov/foia.

Obtained via FOIA by Judicial Watch, Inc.

Provisions of FOIA allow DHS to charge for processing fees, up to $25, unless you seek a waiver of fees. In this instance, because the cost is below the $25 minimum, there is no charge.

If you need any further assistance or would like to discuss any aspect of your request, please contact the analyst below who processed your request and refer to **2017-HQFO-00383**. You may send an e-mail to foia@hq.dhs.gov, call 202-343-1743 or toll free 1-866-431-0486, or you may contact our FOIA Public Liaison in the same manner. Additionally, you have a right to right to seek dispute resolution services from the Office of Government Information Services (OGIS) which mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. You may contact OGIS as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

Maura Busch
Maura Busch
FOIA Program Specialist

Enclosure(s): Responsive Documents, 22 pages

Obtained via FOIA by Judicial Watch, Inc.



DHS Enterprise SOC Daily Operational Status Report Meeting Minutes

Component SOC:	Present	Status
CBP	No	NSTR
DC1	Yes	NSTR
DC2	Yes	NSTR
FEMA	Yes	NSTR
FLETC	Yes	NSTR
FPS	Yes	NSTR
HQ	Yes	NSTR
ICE	Yes	NSTR
NPPD	Yes	NSTR
OIG	No	NSTR
S&T	Yes	NSTR
TSA	Yes	NSTR
USCG	Yes	NSTR
USCIS	Yes	NSTR
USSS	No	NSTR
DHS EWO/NOC	Yes	NSTR
DHS ESOC	Yes	NSTR
DHS Privacy	No	NSTR

Meeting Purpose: To discuss and provide situational awareness of DHS information security operations.		
Facilitator: (b)(6) (b)(6)		
Date: 12/19/2016	Time: 0900-0930	Location: St. Elizabeth/DHS ESOC
Bridge Number: 202-475-4(b)(6)	Confirmation Number: 393 425 88 #	

Obtained via FOIA by Judicial Watch, Inc.

DHS Enterprise SOC Daily Operational Status Report Meeting Minutes

Meeting Summary:
Please see below for the "Meeting Minutes" associated with today's "DHS ESOC Daily Stand-Up" call.

OneNet SOC (DHS ESOC):

Situational Awareness Notes:

- The Department of Homeland Security has been accused by the Georgia Secretary of State, through a formal letter to Secretary Johnson, of conducting an unauthorized penetration test/scan of the "Georgia Secretary of State Firewall" on November 15th, 2016 at 08:43 A.M. The IP address that was logged to this event was the DC2 Proxy 1 IP address (Public: 216.81.81.80; Internal: 10.236.225.141). The IP address of the "Georgia Secretary of State Firewall" was not specified in the letter.
    - Update: The DHS ESOC has begun communicating with the CIO of State of Georgia. The "scanning" event was the result of a FLETC user's Microsoft Office Discovery Protocol sending a packet with the OPTIONS flag to the Secretary of State of Georgia site.
        - Note: Most web servers deny or ignore OPTIONS flag HTTP requests, as it is a depreciated HTTP 1.1 flag. The OPTIONS flag can be used by an attacker to gain information on a web server on what types of request methods it allows. However, in the context of the Georgia case no other suspicious or malicious traffic was found before or after this request.
    - Update 2: The DHS ESOC has received requests from NCCIC and MS-ISAC to investigate other states that have seen "suspicious" activity. If your component receives any State, Local or Tribal (SLT) requests to investigate "suspicious" web traffic from your component or DHS please direct those requests to the NCCIC team and CC the DHS ESOC.
    - Update 3: The DHS ESOC received notice that the Georgia Secretary of State has accused DHS of more "Scanning" activity. We have attached a timeline detailing the date and time of these alleged "scanning" events. The DHS ESOC was able to find logs pertaining to all events after September 12th. However, we are unable to reach back into our logs to find the events that took place on February 2nd, February 28th and May 23rd. The DHS ESOC has found that all "scanning" events happen to coincide with an HTTP "OPTIONS" request to the Georgia site. The Microsoft support team is currently investigating the "OPTIONS" request.
    - Update 4: Microsoft and the ESOC with the assistance of FLETC, were able to confirm that the user non-maliciously copied and pasted elements of the website to an excel document, which triggered the HTTP "OPTIONS" request.

Obtained via FOIA by Judicial Watch, Inc.

DHS Enterprise SOC Daily Operational Status Report Meeting Minutes

MICROSOFT E-MAIL STATEMENT (Unofficial Statement to ESOC):

"DHS contacted Microsoft regarding a concern raised from the State of Georgia (ga.gov) over a DHS workstation triggering a Nexus alert for use of an Options verb request to web site http://verify.sos.ga.gov/verification/. Nexus web traffic data provided to Microsoft support shows the DHS user making normal, expected requests to the website including search requests for "*Search.aspx?facility=Y&SubmitComplaint=Y*", but it is followed by an Options verb request for http://verify.sos.ga.gov/verification/. No further web requests until ~8 hours later which are again the normal requests. These requests are not followed by any Options verb requests.

After looking at the data I do not see requests that look malicious in nature or appear to be attempting to exploit a vulnerability. Additionally the user is known to use copy/'paste special' for data from the webpage to Excel which invokes the Options verb. We have also been able to reproduce the Options verb request by using "right-click Export to Excel" and "right-click Send to OneNote" on the web page, but the user has not reported performing this action."



Timeline of DHS Scanning Activity.pd

***PLEASE DIRECT ALL MEDIA REQUESTS TO THE DHS OFFICE OF PUBLIC AFFAIRS.**

- SEN 2016-11-260 – Wells Fargo performed a third party security assessment against the DHS Enterprise. The assessment found DHS email addresses out in the public and security vulnerabilities on public facing servers. The DHS ESOC recommends notifying the users that their email addresses are out in the public and potentially susceptible to spam and phishing e-mails. The DHS ESOC has attached a security vulnerabilities list to the SEN log on EOC. Please verify these vulnerabilities and develop a plan to remediate them as soon as possible.
    - **The Wells Fargo Team conducted their assessment based off a proprietary tool that uses Open Source methods to collect data on an organization. The DHS ESOC and NCCIC will receive a list of their tools and have a follow-up meeting to discuss their methodology more in-depth at a later date.**
    - **In the coming week, the FISMA Compliance team will provide a way ahead for DHS to remedy the vulnerabilities found during this assessment.**

Obtained via FOIA by Judicial Watch, Inc.



DHS Enterprise SOC Daily Operational Status Report Meeting Minutes

- Please see below for Cyber Hygiene Results Weekly Rollup; view the following site for weekly cyber hygiene reports: http://mgmt-ocio-sp.dhs.gov/ciso/fisma%20reporting/SitePages/FNR%20Cyber%20Hygiene%20Scans.aspx

New ISVM Releases:

There was one (1) ISVM released Friday (12/16/2016):

2016-305-0-B-Apple Multi-Products Vulnerabilities - Apple has released security advisories to address vulnerabilities within Apple Sarfari, Apple macOS, as well as Apple iTunes products, in which successful local/remote exploitation may result in arbitrary code execution, cross-site scripting (XSS), sensitive information disclosure, elevated privileges and/or denial of service.

Research for today:

Nagios vulnerabilities that may result in elevated privileges and/or arbitrary code execution.

ISVM Acknowledgement(s):

- NSTR

ISVM Compliance(s):

- NSTR

Vulnerability Assessment Scans:

- NSTR

US-CERT C-CAR Data Call

- **Binding Operational Directive (BOD-16-02) for all Federal civilian executive branch departments and agencies on Threats to Network Infrastructure Devices has been approved and signed by the DHS Secretary.**

Obtained via FOIA by Judicial Watch, Inc.

DHS Enterprise SOC Daily Operational Status Report Meeting Minutes

- **Perform all actions in the "Solution" sections of the "Technical Annexes" to the NCCIC Analysis Report AR-16-20173 no later than 45 days after issuance of this Directive.**
- **Report to DHS ESOC, either full mitigation or provide a detailed plan of action and milestones explaining the constraints preventing mitigation and the associated compensating controls established no later than 45 days after issuance of this Directive. (11/11/2016)**
- **Provide additional reports or plans of action and milestones every 30 days thereafter until full mitigation is achieved.**
- We are now issuing a high-priority "DHS Enterprise Data Call," in order to obtain a departmental security posture/status related to recently-discovered "Critical" vulnerabilities (affecting Cisco Routers, Cisco Adaptive Security Appliances (ASA) and other vendor firewall devices).
- The following provides general background information and/or context on the three (3) groups of vulnerabilities being addressed via this data call.
  - **Hacking tools targeting firewalls:** A group calling themselves "The Shadow Brokers" claims to have obtained a large-set of hacking tools from the "Equation Group." Said large-set of cyber-weapons (exploits, implants and hacking tools) have targeted firewall devices from vendors such as Cisco, Fortinet, Juniper, WatchGuard, TOPSEC and Huawei.
  - **Cisco ROMMON Integrity:** Based on technical data obtained from focused, in-depth malware analysis, US-CERT was able to identify detection methods/strategies to defend against the involved "Threat Actor."
  - **Cisco Adaptive Security Appliance:** US-CERT received several reports of compromised Cisco Adaptive Security Appliance (ASA) devices. The ASA devices were modified in an unauthorized manner, which resulted in the occurrence of malicious "redirects" (for social engineering/credential-harvesting purposes).
- References:
  - ISVM: 2016-010-0-A-Cisco Adaptive Security Appliance Vulnerabilities
  - ISVM: 2016-010-1-A-Cisco Adaptive Security Appliance Vulnerabilities
  - ISVM: 2016-011-0-A-Fortigate Vulnerability
  - ISVM: 2016-013-0-A-Cisco ASA Clientless SSL VPN Vulnerability
  - ISVM: 2016-016-0-TA-Juniper NetScreen ScreenOS Vulnerability
  - US-CERT Documents:
    - AR-16-20150-Network_Analysis_Report_on_Compromised_Cisco_ASA_Devices.pdf
    - AR-16-20173_The_Increasing_Threat_to_Network_Infrastructure_Devices.pdf
    - CISCO Malware-detection strategy-2.0.pdf

Obtained via FOIA by Judicial Watch, Inc.

- ShadowBroker-EquationGroupHackv1.5.pdf
  - **UPDATE: Ensure to include Estimated Completion Date**
  - **Due weekly, Wednesday 1200 EST**

- **Apple iOS Vulnerability Data Call**
  - **Due Weekly Friday NLT 1600 EST.**
  - Please provide the total number of GFE Apple Mobile Devices, per DHS Component, that have been upgraded to the most current Apple iOS Version.
  - Please provide the total number of GFE Apple Mobile Devices, per DHS Component, that have NOT been successfully upgraded to the most current Apple iOS Version.
  - For those devices that have NOT been properly updated, please provide an explanation as to why this upgrade has not occurred.
  - For those devices that have NOT been properly updated, please provide an Estimated Time to Completion.
  - Reference: 2016-012-0-A-Apple iOS Vulnerabilities

- **Secure Socket Layer (SSL) Version 2 and 3 Vulnerability Data Call:**
  - We have received new guidance from DHS CISO senior leadership for this high-priority "DHS Enterprise Data Call," in order to obtain a departmental security posture status - surrounding a recently-discovered "Critical" vulnerability in devices that utilize "Secure Socket Layer (SSL) versions 2 and 3." If exploited, this vulnerability can result in a successful "cross-protocol attack" being carried-out, potentially resulting in undesirable/unauthorized information disclosures. To meet reporting requirements, the DHS ESOC requires all DHS Component SOC responses weekly on **Friday NLT 1600 EST**.
  - Changes have been updated to the data call and the following information will now be collected:
    - Total Number of Devices Affected
    - Total Number of Devices with available patches/fix (based on vendor(s) releases)
    - Total Number of Devices Remediated
  - Reference: ISVM 2016-053-0-B-OpenSSL DROWN Vulnerabilities

- **Bash Vuln Reporting requirements:**
  - For any remaining unpatched systems, each component will need to determine which systems are internal and external.
  - Numbers will be reported to OMB daily. Please focus on patching external facing systems.
  - Reference: ISVM 2014-009-0-A-GNU Bash Code Injection Vulnerability

- **Cyber Hygiene Vulnerability Scan Report**

Obtained via FOIA by Judicial Watch, Inc.

Homeland Security | Enterprise Security Operations Center

DHS Enterprise SOC Daily Operational Status Report Meeting Minutes

Below you will see the Dashboard for this week's Cyber Hygiene Report. To view more detailed information regarding the vulnerabilities, please see the Scan Results posted on SharePoint.

Make sure to take a look at the Weekly IP Updates tab, specifically at IP's owned by your Component and those marked as having an unknown owner. It would be very much appreciated if you would reply back to me verifying ownership of these IPs. Also, please let me know if you have any updates to contribute to this list, any questions regarding these changes or the current data, or any difficulty accessing the SharePoint link.

If you have any immediate technical questions please reach out to (b)(6)

Cyber Hygiene Vulnerability Scan Report

Start Date:	11/30/2016
End Date:	12/12/2016

Last Report Start:	11/23/2016
Last Report End:	12/4/2016

Current Open Vulnerabilities (1227 Total)

Owner	Severity	Critical (0 Total)				High (7 Total)				Medium (949 Total)				Low (271 Total)				Recently Closed
	Age (in days)	≤ 30 days	31-60 days	61-90 days	> 90 days	≤ 30 days	31-60 days	61-90 days	> 90 days	≤ 30 days	31-60 days	61-90 days	> 90 days	≤ 30 days	31-60 days	61-90 days	> 90 days	
	Unknown (207 Total)	0	0	0	0	0	0	0	2	57	31	0	73	17	16	0	11	62
	CBP (88 Total)	0	0	0	0	0	0	0	0	7	1	2	68	3	6	0	1	11
	CIS (61 Total)	0	0	0	0	0	0	0	0	5	0	3	42	3	8	0	0	5
	FEMA (170 Total)	0	0	0	0	0	0	0	5	21	5	2	95	10	11	0	21	40
	FLETC (0 Total)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	HQ (361 Total)	0	0	0	0	0	0	0	0	65	7	12	209	11	33	0	24	35
	ICE (3 Total)	0	0	0	0	0	0	0	0	1	0	0	0	2	0	0	0	1
	NPPD (8 Total)	0	0	0	0	0	0	0	0	2	0	1	3	0	2	0	0	10
	OIG (4 Total)	0	0	0	0	0	0	0	0	1	0	0	2	1	0	0	0	0
	S&T (24 Total)	0	0	0	0	0	0	0	0	17	0	0	5	1	1	0	0	1
	TSA (253 Total)	0	0	0	0	0	0	0	0	49	15	4	103	27	38	0	17	14
	USCG (48 Total)	0	0	0	0	0	0	0	0	2	4	3	32	1	3	0	3	14
	USSS (0 Total)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Obtained via FOIA by Judicial Watch, Inc.

There continues to be an incomplete reflection of component scanning activity as indicated by the representation of opened/closed/pending VAT records within EOCOnline. The DHS ESOC VAT continues to request for VAT record creation within the EOCOnline Portal reflecting component's scanning activities. DHS ESOC analysts routinely receive requests from components for assistance with reporting/investigating unexpected network activity, which could be perceived as potentially malicious traffic. A simple query into the VAT records would afford our team with the ability to quickly diffuse any unnecessary alarm(s), or quickly respond appropriately to bad-actors attempting to compromise the network.

2.3.4.1 Component Vulnerability Assessments

> *"Components shall prepare schedules including complete coverage of all systems and shall conduct monthly credentialed vulnerability assessments. The schedules must be provided to the DHS VMB through the Government provided system of record and may be updated as often as necessary. Schedules, updates, and assessment and remediation results will be provided to DHS VMB no less than quarterly and upon request in periodic data calls. Each scan shall be posted in the Government-provided system of record as an in-process scan for each Component. Scan results shall be uploaded into Enterprise Vulnerability Management System (EVMS). Components shall declare any inability to perform vulnerability assessments, analysis, penetration testing or reporting to the DHS VMB and arrange for an alternate solution."*
>
> Source: 4300A, Attachment O, Section 2.3.4.1

For further inquiries regarding ISVM notifications or vulnerabilities assessments, please contact DHS_SOC_VAT (b)(6)

DHS ESOC Threat Intelligence

NSTR

DHS ESOC IDS:

Obtained via FOIA by Judicial Watch, Inc.



DHS Enterprise SOC Daily Operational Status Report Meeting Minutes

NSTR

DHS ESOC Engineering:

NSTR

DHS ESOC E-mail Team:

2016-12-160 Users: 1 (USCIS 1)

Subject: "incoming report"

Sender: (b)(6)

Date: 12/16

Type: Credential Harvesting

Attachment: NA

Callbacks: hxxp://rdastudio[d]net/rage/ayo1/ayo1/index[d]html

2016-12-161 Users: search underway…

Subject: [WARNING: MESSAGE ENCRYPTED][SPAM]*xxxx

Sender: search underway…

Date: 12/18

Type: Malicious Logic

Attachment: *****.zip

Callbacks: hl3gj7zkxjvo6cra.onion[.]to

DHS ESOC Incident Response (IR):

SENS: 10

2016-12-161 ML-Phishing-Campaign

2016-12-135 MU-CBP-DHS

2016-12-160 credential Phishing

Obtained via FOIA by Judicial Watch, Inc.

2016-12-157	S&T_STCS_Domain_Admin
2016-12-152	Investigation Un
2016-12-158	Investigation Un
2016-12-159	MU-CBP-DHS
2016-12-154	IU-CBP-DHS
2016-12-153	USCG Recruiting Command
2016-12-155	IM48253

Incidents: 8

2016-12-075	MU-CBP-DHS
2016-12-074	Misuse
2016-12-073	Misuse
2016-12-072	Misuse
2016-12-071	USCG Recruiting Command
2016-12-070	PII Non-Technical Spill
2016-12-069	PII Non-Technical Spill
2016-12-068	MU-CBP-DHS

Blocks: 5

rdastudio[.]net

The DHS ESOC received Fire Eye alerts for phishing email from sender "sawerning17@benton.k12.ia.us" using subject line "incoming report" was delivered to a DHS user.The email solicits the user to click a link to see the attached document. OOB analysis shows the link "hxxp://rdastudio[d]net/rage/ayo1/ayo1/index[d]html" opens a page asking for email username and password Recommending blocking the domains to enhance DHS security.

Obtained via FOIA by Judicial Watch, Inc.

118[.]193[.]243[.]149

171[.]83[.]99[.]175

184[.]28[.]218[.]190

23[.]76[.]205[.]110

US-CERT reported to DHS ESOC on December 16th, 2016 of known MalSpam delivering Locky ransomware. DHS ESOC recommends blocking associated IPs, in order to strengthen our security posture.

Obtained via FOIA by Judicial Watch, Inc.

From:	DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
SentVia:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
To:	"/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; "CTR ESOC Leads </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS SOC LEADS GMLca3>"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
CC:	"/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC GWO476"; "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"
Subject:	Shift Pass Down Report - Sunday Night Shift - December 18, 2016
Date:	2016/12/19 06:57:29
Priority:	Normal
Type:	Note

Shift Pass Down Report - Sunday Night Shift - December 18, 2016

~~U/FOUO~~

High Profile SENs/Incidents/CRs (Include The SEN/INC/CR # and short description):

- • * **State of Georgia update:**
  DHS initiated an investigation into allegations from the Georgia Secretary of State (GASOS) Brian Kemp that DHS was attempting to penetrate the Georgia Secretary of State's firewall. DHS identified that the event in question originated from a FLETC-based Physical Security Contract Manager. The user uses the GASOS website to validate that employees have the licenses required to be armed guards. Once the user finds the information he needs, he copies and pastes it to a Microsoft Excel document. Microsoft confirmed today this action invokes the "HTTP OPTIONS" command. Data provided by GASOS CIO shows that their Managed Service Provider generated an automated alert based on their firewalls detecting the "HTTP Options" command. Microsoft's assessment corroborates DHS' technical assessment and the user's explanation.
  - ➢ **DHS ESOC is still awaiting additional information from GA CIO and ESOC(Boyden) has briefed the Hill.**
- • * **State of Alaska update**:
  Confirmed this activity was a NPPD employee investigating twitter reports of compromise on an AK Election System, as part of his normal duties. Reported this back to the NCCIC, NCATS, and MS-ISAC teams.
- • * **State of Oregon update:**
  OregonSecretary of State inquired why they observed the same DHS IP reported by GASOS visiting their website. After engaging with DHS, Oregon agreed there was nothing suspicious and closed the investigation. Reported this to NCCIC, NCATS, and MS-ISAC.
- • * **State of Kentucky update:**
  Normal web traffic from DHS. Reported this to (b)((b)(6) and Jeanette Manfra.
- • * **State of West Virginia update:**

Obtained via FOIA by Judicial Watch, Inc.

Normal web traffic from DHS. (b)(will get additional information from WV so that ESOC can investigate.

- • * **Princess Cruise Line latest update:**
  ESOC concluded that suspicious activity reported to DHS by Princes Cruises was normal web traffic coming from different Components. This determination was made by reviewing DHS' own logs; ESOC did not receive any logs from Princess Cruises to review.
- • * SEN 2016-12-133: ICE DMA captured RAM dump for the potentially infected host. Email has been sent to ESOC DMA to arrange transfer of the file.
- • * SEN 2016-12-159 & 2016-12-135 & 2016-12-066: DO NOT ESCALATE until ESOC (b)(6) discuss them with GWO (b)(6)
- • * FEMA Significant Incident 2016-12-029: Continue working with FEMA on this incident and periodically review Incident's log and email chains.

Next Shift Issues/Events to Work :

- • * Continue working on Web Requests. Please carefully read each WRs for proper business justification and component SOC/CISO assessments for before approving them.
- • * SEN 2016-12-161 – work the email from ICE SOC in the DHS ESOC inbox

On-Going/Future ISSUES/Events:

- • * **DC3 Field Trip at DC3 Facility- Presentations will be heavily focused on DMA and FO – January 19th.**
- • * FireEye tool still having issue with Sender's name: Security Engineering Team is working the issue. Still awaiting a response.
- • * INC 2016-10-096: CBP SSO is still unable to determine the OCA of the document but will contact the NSA next. Workstation remediation actions has begun with DHS I&A Dep CISO's permission.

Web-Request (Mission Critical):

- When dealing with Social Media WR ensure that Riley Dean (DHS Privacy Officer) is engaged, he has requested that all WR are routed to him.

Upcoming Events

- • * DHS ESOC Passdown meeting for Back half Day/Night shifts has been re-schedule. TBD.

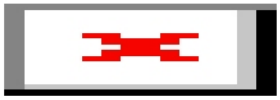
Situation Awareness

- • * NSTR

V/r,

(b)(6) (b)(6)
Shift lead, SOC – Incident Handling
General Dynamics Information Technology (GDIT)
Supporting the Department of Homeland Security (DHS)
DHS Enterprise Security Operations Center (ESOC)
MGMT/OCIO/CISO/ESOC

Obtained via FOIA by Judicial Watch, Inc.



dhs_esoc_2_info

Sender:	DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) DHS.GOV3A5>; (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
Recipient:	"/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; "CTR ESOC Leads </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS SOC LEADS GMLca3>"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=(b)(6) 3a5>"; "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC GWO476"; "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"
Sent Date:	2016/12/19 06:57:28
Delivered Date:	2016/12/19 06:57:29

Obtained via FOIA by Judicial Watch, Inc.

From:	Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=BOYDEN.ROHNER>
To:	(b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Subject:	FW: Georgia Slide
Date:	2016/12/30 13:25:06
Priority:	Normal
Type:	Note

Can you take a look for us please?

From: Schneck, Dr. Phyllis
Sent: Friday, December 30, 2016 6:11:19 PM
To: Rohner, Boyden; (b)(6) (b)(6)
Cc: (b)(6)
Subject: FW: Georgia Slide

This should be what we need – thoughts?

From: (b)(6) (b)(6)
Sent: Friday, December 30, 2016 11:05 AM
To: Schneck, Dr. Phyllis (b)(6)
Subject: Georgia Slide

Sender:	Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=BOYDEN.ROHNER>
Recipient:	(b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Sent Date:	2016/12/30 13:25:06

Obtained via FOIA by Judicial Watch, Inc.

Georgia SoS/DHS Intrusion Case
Microsoft Findings

Washington, DC | December 16, 2016

Microsoft

Obtained via FOIA by Judicial Watch, Inc.

Georgia SoS/DHS Intrusion Case

Microsoft Findings

- **Technical Explanation:** DHS contacted Microsoft regarding a concern raised from the State of Georgia (ga.gov) over a DHS workstation triggering a security alert, by their scanning tool, manufactured by Nexus, for use of an Options Verb* request to web site http://verify.sos.ga.gov/verification/ . The State of Georgia (ga.gov) uses the Nexus software to scan for vulnerabilities and exploits. The DHS Enterprise Security Operations Center (ESOC) performed additional analysis on this event and found that the identified request was attributed to a standard Microsoft Protocol**. This is a fairly typical request of Microsoft Office Applications to check web server compatibility. The ESOC requested that Microsoft conduct further investigation to confirm that the system request, made by the DHS user, was normal and non-malicious.

STRATEGY □ CONSULTING □ SUPPORT

- **Investigation:** Microsoft deployed Cyber Support Engineering resources to investigate the security alert. DHS ESOC provided logs to Microsoft for review, including logs from the workstation that initiated the request. A joint team of Microsoft Engineers and DHS Engineers convened to review the data and attempt to recreate the communication protocol in question.

- **Findings**: Microsoft reviewed the data, conducted interviews and reproduced the request. Microsoft did not observe any evidence that the referenced requests were malicious in nature. All indications are these were normal requests made by a standard Microsoft Protocol. The DHS employee accessed the http://verify.sos.ga.gov/verification/ site and copied data from the search results to and excel file. This generated a false positive from the page and the user using the "special" copy function that generates an Option Verb request.

- **Next Steps:** Microsoft recommends that State of Georgia (ga.gov) contact their scanner provider (Nexus) and have the false positive corrected for this scenario.

*This is an HTTP protocol that asks the server what it supports or is capable of. For example "is the server capable of opening an excel spreadsheet". It does not initiate resource requests, action or retrieval from the server.

**"Understanding Microsoft Office Protocol Discovery" https://support.microsoft.com/en-us/kb/838028

Obtained via FOIA by Judicial Watch, Inc.

Microsoft

© 2014 Microsoft Corporation. All rights reserved.

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
To:	Non Responsive </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
Subject:	RE: Preliminary update on GASOS
Date:	2016/12/16 11:59:54
Priority:	Normal
Type:	Note

Thank you for the tip (b)(6) Hope that last one meshes better with what was needed.

It was probably still a little long winded. I'll have to work on making these more succinct and consumable for executive notifications.

v/r

(b)(6) (b)(6) PMP, CISSP, GCIA, GCIH, Sec+, ITILv3
ESOC Operations Manager
Department of Homeland Security (DHS) Enterprise Security Operations Center (ESOC)
MGMT/OCIO/CISO/SOC
BB: 202-309-(b)(6)
Office: 202-372-(b)(6)
DHS SOC: 1-877-347-(b)(6) Option 2

From: (b)(6)
Sent: Friday, December 16, 2016 10:56 AM
To: (b)(6) (b)(6) (b)(6)
Subject: FW: Preliminary update on GASOS

FYI. Please use the lens of Press Release and senior leaders.

From: Etzel, Jeanne
Sent: Friday, December 16, 2016 10:54 AM
To: (b)(6) (b)(6)
Subject: RE: Preliminary update on GASOS

When this gets published in the 4:00, don't say "lack of logs" say something about logs are maintained for xx days and the events in question occurred xx days ago therefore our logs were overwritten per our standard retention policy.

Thank you,

Jeanne Etzel
Principal Deputy Chief Information Officer (Acting)
Department of Homeland Security

Obtained via FOIA by Judicial Watch, Inc.

202-447-(b)(6)

From: (b)(6) (b)(6)
Sent: Friday, December 16, 2016 10:51 AM
To: Fulghum, Chip (b)(6) Non Responsive (b)(6)
Etzel, Jeanne (b)(6)
Subject: FW: Preliminary update on GASOS

This is raw. I'll provide more information at the 4 pm update.

From: (b)(6) (b)(6)
Sent: Friday, December 16, 2016 10:49 AM
To: (b)(6) (b)(6) (b)(6)
Cc: Rohner, Boyden (b)(6) (b)(6) (b)((b)(6) (b)(6) (b)(6) (b)(6)
Subject: RE: Preliminary update on GASOS

Mr. (b)(6)

Please see below.

With regards to Georgia we have confirmed with that the traffic is legitimate and expected behavior along with verification from Microsoft. This traffic is not only from FLETC, but also includes ICE-CIS and FEMA.

- An interview was conducted with the FLETC user who generated the first traffic on November 15th and relayed his steps while he was on Georgia's SOS site. This included copy and pasting license plate numbers for law enforcement personnel to do their lookups. This copy and paste invokes the web traffic that Georgia's SOS identified to be suspicious.
- DHS ESOC regenerated traffic that matched this users activity and matched the logs directly up with the traffic that occurred on November 15th.
- Microsoft has validated our logs, the logs from FLETC and confirmed this traffic to be normal web behavior that would occur should you copy and paste from a website into a Microsoft office product.
    - Each of the other timestamps where we had logs available also matched with this same normal web behavior.

With regards to the other 10 timestamps, given that there are 14 IPs with over 350,000 users behind them, we have identified different components who have caused the same traffic as the FLETC user. Those components are broken down below.

- At this time, we cannot validate users with ease for these past timestamps due to DHCP and the lack of Authentication logs. Thus an interview was not done for these events.
    - Once we begin authenticating through the Proxies, we will have matching username and can proceed in the future

- September 12, 2016 12:52:32 EDT (11:52 CDT)

Obtained via FOIA by Judicial Watch, Inc.

  - Host 10.61.22.222 (**ICE-CIS**)*
- September 28, 2016 08:54:15 EDT (07:54 CDT)
  - Host 10.56.189.94 (**ICE-CIS**)*
- October 3, 2016 11:41:32 EDT (10:41 CDT)
  - Host 10.101.194.178 (**ICE-CIS**)*
- October 6, 2016 11:14:16 EDT (10:14 CDT)
  - Host 10.32.82.42 (**FEMA**)
- November 7, 2016 13:15:43 EST (12:15 CST)
  - Host 10.56.189.65 (**ICE-CIS**)*
- November 8, 2016 08:35:21 EST (07:35 CST)
  - Host 10.243.15.188 (**FLETC**)

- May 23, 2016 08:42 CDT
  - Unknown component (verified similar activity) – alternate logs do not provide component information this far back
- February 28, 2016 13:19 CST
  - Unknown component (verified similar activity) – alternate logs do not provide component information this far back
- February 2, 2016 13:03 CST
  - Unknown component (verified similar activity) – alternate logs do not provide component information this far back

*note: The "ICE-CIS" components are listed due to ICE and CIS sharing much of their IP space.

v/r

(b)(6) (b)(6) PMP, CISSP, GCIA, GCIH, Sec+, ITILv3
ESOC Operations Manager
Department of Homeland Security (DHS) Enterprise Security Operations Center (ESOC)
MGMT/OCIO/CISO/SOC
BB: 202-309-(b)(6)
Office: 202-372-(b)(6)
DHS SOC: 1-877-347-(b)(6)

From: (b)(6)
Sent: Friday, December 16, 2016 10:30 AM
To: (b)(6) (b)(6) (b)(6)
Cc: Rohner, Boyden (b)(6) (b)(6) (b)((b)(6)
Subject: Preliminary update on GASOS

Can you shoot me a quick update on what was just discussed with the USM. I need to share that with him and Luke in written form.

Sender:	(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Recipient:	"Eisensmith, Jeffrey </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP

Obtained via FOIA by Judicial Watch, Inc.

	(FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
Sent Date:	2016/12/16 11:59:54

Obtained via FOIA by Judicial Watch, Inc.

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Privacy Office, Mail Stop 0655

February 28, 2019

SENT BY ELECTRONIC MAIL TO: bmarshall@judicialwatch.org

William F. Marshall
Senior Investigator
Judicial Watch
425 Third Street, SW, Suite 800
Washington, DC 20024

Re: 2017-HQFO-00383

Dear Mr. Marshall:

This is an interim response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated January 26, 2017, and received by this office on February 14, 2017. You are seeking any and all records relating to reported cyberattacks against the Georgia Secretary of State's information network involving DHS and/or its employees or contractors, including but not limited to investigative reports, memoranda, correspondence and communications (Date Range for Record Search: from 10/1/2016 To 2/14/2017).

On March 30, 2018, our office forwarded to you an acknowledgement letter that in addition to our office conducting a search for records, that we transferred your request to the OIG FOIA Office for their review and direct response to you.

On December 7, 2018, our office sent our first interim response of 22 pages from our search for records from the Office of the Chief Information Officer (CIO) and this search yielded over 1,400 pages of records. Due to the volume of this record set, you agreed that you would accept rolling or interim responses from our office.

As such, for our second interim response, we are forwarding to you 219 pages. Of those pages, I have determined that 141 pages of the records are releasable in their entirety, 78 pages are partially releasable, pursuant to FOIA Exemption 6.

FOIA Exemption 6 exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right to privacy. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

Obtained via FOIA by Judicial Watch, Inc.

You have a right to appeal the above withholding determination. Should you wish to do so, you must send your appeal and a copy of this letter, within 90 days of the date of this letter, to: Privacy Office, Attn: FOIA Appeals, U.S. Department of Homeland Security, 245 Murray Lane, SW, Mail Stop 0655, Washington, D.C. 20528-0655, following the procedures outlined in the DHS FOIA regulations at 6 C.F.R. Part 5 § 5.8. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS FOIA regulations are available at www.dhs.gov/foia.

Provisions of FOIA allow DHS to charge for processing fees, up to $25, unless you seek a waiver of fees. In this instance, because the cost is below the $25 minimum, there is no charge.

After you review the records from this second interim response, please advise if you are still interested in our office reviewing the balance of the records.

If you need any further assistance or would like to discuss any aspect of your request, please contact the analyst below who processed your request and refer to **2017-HQFO-00383**. You may send an e-mail to foia@hq.dhs.gov, call 202-343-1743 or toll free 1-866-431-0486, or you may contact our FOIA Public Liaison in the same manner. Additionally, you have a right to right to seek dispute resolution services from the Office of Government Information Services (OGIS) which mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. You may contact OGIS as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

James V.M.L. Holzer, I

James V.M.L. Holzer
Deputy Chief FOIA Officer

Enclosure(s): Responsive Documents, 219 pages

Obtained via FOIA by Judicial Watch, Inc.

From:	DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=SOCDHSONENET.CBP.DHS.GOV3A5>
SentVia:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>
To:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"
CC:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6))/CN=RECIPIENTS/CN=(b)(6) 4a0>"
Subject:	RE: (Easy) Request assistance for DHS
Date:	2016/12/09 22:26:30
Priority:	Normal
Type:	Note

Hello Boyden ,

Yes it does corroborate with (b)(6) findings.

Please see below for comparison.

Sample Log from DHS Splunk:

2016-11-08 13:35:21 62 10.243.15.188 10.76.225.140 50.232.155.145 - - FLETC 200 TCP_NC_MISS OBSERVED 233 260 237 206 OPTIONS http verify.sos.ga.gov 80 /verification/stylesheets/ - - - "Microsoft Office Protocol Discovery" "Government/Legal" - - 42 "none" "none" 58965 38084

Sample Log From the Attachment

Dec 9 21:33:52 10.66.218.134 CEF:0|Blue Coat|Proxy SG||TCP_ERR_MISS|TCP_ERR_MISS|High| eventId=17656548 app=https in=811 out=204 categorySignificance=/Informational/Error categoryBehavior=/Execute/Response categoryDeviceGroup=/Proxy catdt=Firewall categoryOutcome=/Failure categoryObject=/Host/Resource/File art=1481337227843 cat=main deviceSeverity=503 act=PROXIED rt=1481337206000 shost=107.77.202.117 src=107.77.202.117 sourceZoneURI=/All Zones/ArcSight System/Dark Address Space Zones/100.0.0.0-107.255.255.255 (IANA) dhost=10.66.192.37 dst=10.66.192.37 destinationZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 request=https://www.ncjrs.gov/pdffiles1/nij/grants/ requestMethod=OPTIONS requestClientApplication=Microsoft Office Protocol Discovery cs1=- cs2=none cn1=0 c6a4=fe80:0:0:0:ba2a:72ff:fece:4b4c cs1Label=x-risk-category cs2Label=sc-filter-category cs3Label=r-supplier-ip cs4Label=cs-categories cs5Label=x-bluecoat-application-operation cs6Label=cs-auth-group cn1Label=x-risk-score c6a4Label=Agent IPv6 Address ahost=pidsenammp1c004.monitormanage.cjis

Obtained via FOIA by Judicial Watch, Inc.

agt=10.66.218.135 agentZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 av=7.1.7.7600.0 atz=America/Boise aid=3y0HaD1MBABCAwmrLrtFRag\=\= at=bluecoat_ng_file dvchost=10.66.192.37 dvc=10.66.192.37 deviceZoneURI=/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255 dtz=America/Boise deviceProcessName=SG-HTTPS-Reverse-Proxy-Service requestProtocol=https requestUrlAuthority=www.ncjrs.gov requestUrlHost=www.ncjrs.gov requestUrlFileName=/pdffiles1/nij/grants/ _cefVer=0.1 ad.s-hierarchy=- ad.x-virus-id=- ad.time-taken=694
Dec

requestMethod=OPTIONS requestClientApplication=Microsoft Office Protocol Discovery

---

From: Rohner, Boyden
Sent: Friday, December 9, 2016 9:58 PM
To: DHS ESOC <DHSESOC@hq.dhs.gov>; (b)(6) >; (b)(6) (b)(6)
Cc: (b)(6) >
Subject: FW: (Easy) Request assistance for DHS

FYI-

Does this corroborate (b)(6) findings about dhs's 1800 "option" queries in 3 hours?

From: (b)(6)
Sent: Saturday, December 10, 2016 2:47:01 AM
To: Rohner, Boyden
Subject: RE: (Easy) Request assistance for DHS

Ok,

Here's what we have so far. Not sure if it supports what you guys are looking at but we're seeing some of the activity you describe.

From: Rohner, Boyden [mailto:(b)(6) @HQ.DHS.GOV]
Sent: Friday, December 9, 2016 7:27 PM
To: (b)(6) (JMD) <(b)(6) >
Subject: RE: (Easy) Request assistance for DHS

Thank you!

Obtained via FOIA by Judicial Watch, Inc.

From: (b)(6)
Sent: Saturday, December 10, 2016 12:15:08 AM
To: Rohner, Boyden
Cc: (b)(6) DHS ESOC
Subject: RE: (Easy) Request assistance for DHS

I'll have our team take a look at this and get back to you.

Thanks,

(b)(6)
Chief, Justice Security Operations Center (JSOC)
US Department of Justice
202-357-0198

From: Rohner, Boyden [mailto:(b)(6)
Sent: Friday, December 9, 2016 6:36 PM
To: (b)(6) (JMD) <(b)(6)>
Cc: (b)(6) DHS ESOC <DHSESOC@hq.dhs.gov>
Subject: (Easy) Request assistance for DHS

Good afternoon, (b)(6) –

(b)(6) suggested I reach out to you for some assistance on an investigation we're conducting. We're investigating some claims by the State of Georgia that we've been scanning their website. A review of our logs indicates that Microsoft Office generates an HTTP.request.method=OPTIONS which is the event that triggered the suspicion by the State of GA.

When we pull our logs over a three hour period, we see that we have about 1800 similar requests. Do you see this type of network traffic regularly as well? Specifically, can you search your proxy logs to confirm the following traffic pattern when a user views a Microsoft Office file from a website? Before the get request, the user's browser would send an HTTP request method =OPTIONS and user agent string ="Microsoft Office discovery protocol". Here's an example of what we're seeing:



cid:image001.jpg@01D25265.91CF9280

Thank you very much for your help. Please email me or (b)(6) (copied) if you have any questions.

Boyden Rohner

Obtained via FOIA by Judicial Watch, Inc.

Director, Cybersecurity Operations
DHS
(202) 657-(b)(6)

Sender:	DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=SOCDHSONENET.CBP.DHS.GOV3A5>; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>
Recipient:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"
Sent Date:	2016/12/09 22:26:29
Delivered Date:	2016/12/09 22:26:30

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
To:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6); (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"
CC:	(b)(6) /O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6); '(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; '(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; '(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; '(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; '(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; '(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; '(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"
Subject:	RE: State of Alaska Log Data
Date:	2016/12/10 00:01:07
Priority:	Normal
Type:	Note

ALCON ,

SoureFire rules for a non-standard traffic going to Alaska (158.145.240[.]103) and Georgia (50.232.155[.]145) IPs has been created for monitoring.

From: (b)(6) (CTR)
Sent: Friday, December 9, 2016 6:57 PM
To: (b)(6) (CTR) (b)(6); (b)(6) (CTR) (b)(6); (b)(6) <(b)(6)>; DHS ESOC Analysts <DHSESOCAnalysts@hq.dhs.gov>
Cc: (b)(6) (CTR) (b)(6)

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Id	Subject	Next Action Owner	Original Requester	Created	Last Action	Severity	Status	Time Spent	External Ticket
23389418	Department of Homeland Security Scanning Activity	(b)(6)	SOC Staff	Nov 15, 2016 08:54	Nov 15, 2016 09:11	Medium	Open	None	

Ticket Detail	
Date	Nov 15, 2016 08:54
Ticket ID	23389418
Client	Secretary of State, Georgia
Summary	Department of Homeland Security Scanning Activity
Severity	Medium
Originator	SOC Staff
Next Action Owner	(b)(6)
Service Category	Incident
Security	Yes
Affected Assets	Public/50.232.155.128
15, Nov 2016 09:11:35	**automation** **EventLinking-VLDB**

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

DHS IP Address

Target- SOS IP address

Logs containing source IP 21 6.81.81.80 or destination IP 50.232.155.145 from origina l event with timestamp 2016/ 11/15 13:43:25 +/- 5 minutes .

Nov 15 08:47:59 10.1.0.2 1,2016/11/15 08:47:59,001801 015967,TRAFFIC,end,1,2016/11 /15 08:47:59,209.67.78.48,50 .232.155.145,209.67.78.48,10 .250.0.10,inbound-web-browsi ng,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15 08:47:59,30287,1,38032,8 0,38032,80,0x40001c,tcp,allo w,55016,10883,44133,80,2016/ 11/15 08:47:15,28,government ,0,2816313004,0x0,US,US,0,40 ,40,tcp-rst-from-server,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:47:58 10.1.0.2 1,2 016/11/15 08:47:58,001801015 967,TRAFFIC,start,1,2016/11/ 15 08:47:58,192.35.47.1,50.2 32.155.145,192.35.47.1,10.25 0.0.10,inbound-web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15 08:47:58,41407,1,18011,80,1 8011,80,0x400000,tcp,allow,1 189,1123,66,4,2016/11/15 08: 47:58,0,any,0,2816312976,0x0 ,US,US,0,3,1,n/a,0,0,0,0,,AT L-PAN-01,from-policy
Nov 15 08:47:58 10.1.0.2 1,2016/11/ 15 08:47:58,001801015967,TRA FFIC,end,1,2016/11/15 08:47: 58,68.156.159.10,50.232.155. 145,68.156.159.10,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell - secureworks,2016/11/15 08:4 7:58,56156,1,35074,80,35074, 80,0x40001c,tcp,allow,14617, 1789,12828,27,2016/11/15 08: 47:42,0,government,0,2816312 971,0x0,US,US,0,15,12,tcp-fi n,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:47:59 10.1.0 .2 1,2016/11/15 08:47:59,001 801015967,TRAFFIC,start,1,20 16/11/15 08:47:59,64.179.192 .42,50.232.155.145,64.179.19 2.42,10.250.0.10,inbound-web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15 08:47:59,31405,1, 12764,80,12764,80,0x400000,t cp,allow,1180,1114,66,4,2016 /11/15 08:47:58,0,any,0,2816 312985,0x0,US,US,0,3,1,n/ a,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:47:59 10.1.0.2 1,2016/11/15 08:47:59,001801 015967,TRAFFIC,end,1,2016/11 /15 08:47:59,205.173.105.205 ,50.232.155.145,205.173.105. 205,10.250.0.10,inbound-web- browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2 016/11/15 08:47:59,24150,1,4 1564,80,41564,80,0x40001a,tc p,allow,2202,623,1579,7,2016 /11/15 08:47:32,11,governmen t,0,2816313016,0x0,US,US,0,4 ,3,tcp-rst-from-client,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:47:58 10.1.0.2 1,20 16/11/15 08:47:58,0018010159 67,TRAFFIC,end,1,2016/11/15 08:47:58,64.85.77.7,50.232.1 55.145,64.85.77.7,10.250.0.1 0,inbound-web-browsing,,,web

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

-browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4
7:58,38532,1,56586,80,56586, 80,0x40001c,tcp,allow,10858, 1881,8977,22,2016/11/15 08:4
7:39,3,government,0,28163129 70,0x0,US,US,0,12,10,tcp-rst -from-client,0,0,0,0,,ATL-PA
N-01,from-policy
Nov 15 08:4 7:59 10.1.0.2 1,2016/11/15 0 8:47:59,001801015967,TRAFFIC ,end,1,2016/11/15
08:47:59,6 6.192.63.2,50.232.155.145,66 .192.63.2,10.250.0.10,inboun d-web-browsing,,,web-
browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew orks,2016/11/15
08:47:59,553 48,1,59229,80,59229,80,0x400 01c,tcp,allow,76547,17084,59 463,70,2016/11/15
08:46:35,6 8,government,0,2816313018,0x 0,US,US,0,26,44,tcp-fin,0,0, 0,0,,ATL-PAN-01,from-
policy
Nov 15 08:47:59 10.1.0.2 1,2 016/11/15 08:47:59,001801015 967,TRAFFIC,end,1,2016/11/15
08:47:59,205.173.105.205,50 .232.155.145,205.173.105.205 ,10.250.0.10,inbound-
web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-
secureworks,2016 /11/15 08:47:59,48824,1,4685 1,80,46851,80,0x40001a,tcp,a
llow,2202,623,1579,7,2016/11 /15 08:47:43,0,government,0, 2816313031,0x0,US,US,0,4,3,t cp-
rst-from-client,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:47:59 10.1.0.2 1,2016/1 1/15 08:47:59,001801015967,T RAFFIC,start,1,2016/11/15
08 :47:59,64.179.192.42,50.232. 155.145,64.179.192.42,10.250 .0.10,inbound-
web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-
secureworks,2016/11/15 08:47:59,47672,1,41703,80,41 703,80,0x400000,tcp,allow,11
81,1115,66,4,2016/11/15 08:4 7:59,0,any,0,2816313052,0x0, US,US,0,3,1,n/a,0,0,0,0,,ATL -
PAN-01,from-policy
Nov 15 0 8:47:59 10.1.0.2 1,2016/11/1 5 08:47:59,001801015967,TRAF FIC,end,1,2016/11/15
08:47:5 9,12.167.43.50,50.232.155.14 5,12.167.43.50,10.250.0.10,i nbound-web-
browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se
cureworks,2016/11/15 08:47:5 9,196682,1,52757,80,52757,80 ,0x40001c,tcp,allow,31487,20
30,29457,42,2016/11/15 08:47 :43,0,government,0,281631303 8,0x0,US,US,0,20,22,tcp-fin,
0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:47:58 10.1.0.2 1,2016/11/15 08:47:58,00180 1015967,TRAFFIC,start,1,2016 /11/15
08:47:58,192.35.47.1, 50.232.155.145,192.35.47.1,1 0.250.0.10,inbound-web-brows
ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1
1/15 08:47:58,40935,1,47867, 80,47867,80,0x400000,tcp,all ow,1189,1123,66,4,2016/11/15
08:47:58,0,any,0,2816312975 ,0x0,US,US,0,3,1,n/a,0,0,0,0 ,,ATL-PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:59 10.1.0.2 1,2016 /11/15 08:47:59,001801015967 ,TRAFFIC,start,1,2016/11/15 08:47:59,64.179.192.42,50.23 2.155.145,64.179.192.42,10.2 50.0.10,inbound-web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5 08:47:59,37619,1,64667,80, 64667,80,0x400000,tcp,allow, 1181,1115,66,4,2016/11/15 08 :47:58,1,any,0,2816313051,0x 0,US,US,0,3,1,n/a,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:47:58 10.1.0.2 1,2016/11 /15 08:47:58,001801015967,TR AFFIC,start,1,2016/11/15 08: 47:58,192.35.47.1,50.232.155 .145,192.35.47.1,10.250.0.10 ,inbound-web-browsing,,,web-browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell- secureworks,2016/11/15 08:47 :58,45706,1,2856,80,2856,80, 0x400000,tcp,allow,1188,1122 ,66,4,2016/11/15 08:47:58,0, any,0,2816312961,0x0,US,US,0 ,3,1,n/a,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:47:57 10.1.0.2 1,2016/11/15 08:47 :57,001801015967,TRAFFIC,sta rt,1,2016/11/15 08:47:57,12. 167.43.50,50.232.155.145,12. 167.43.50,10.250.0.10,inboun d-web-browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew orks,2016/11/15 08:47:57,359 70,1,52759,80,52759,80,0x400 000,tcp,allow,986,912,74,4,2 016/11/15 08:47:56,0,any,0,2 816312874,0x0,US,US,0,3,1,n/ a,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:47:57 10.1.0 .2 1,2016/11/15 08:47:57,001 801015967,TRAFFIC,end,1,2016 /11/15 08:47:57,209.67.78.57 ,50.232.155.145,209.67.78.57 ,10.250.0.10,inbound-web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:47:57,37059,1,4025 3,80,40253,80,0x40001c,tcp,a llow,7940,2652,5288,21,2016/ 11/15 08:47:37,4,government, 0,2816312835,0x0,US,US,0,14, 7,tcp-rst-from-client,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:47:57 10.1.0.2 1,201 6/11/15 08:47:57,00180101596 7,TRAFFIC,end,1,2016/11/15 0 8:47:57,108.66.253.68,50.232 .155.145,108.66.253.68,10.25 0.0.10,inbound-web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15 08:47:57,47496,1,60777,80,6 0777,80,0x40001c,tcp,allow,1 77705,13397,164308,178,2016/ 11/15 08:46:58,43,government ,0,2816312868,0x0,US,US,0,60 ,118,tcp-rst-from-client,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:47:57 10.1.0.2 1, 2016/11/15 08:47:57,00180101 5967,TRAFFIC,end,1,2016/11/1 5 08:47:57,64.85.97.251,50.2 32.155.145,64.85.97.251,10.2 50.0.10,inbound-web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5 08:47:57,11964,1,56654,80, 56654,80,0x40001c,tcp,allow,

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

35061,3460,31601,56,2016/11/ 15 08:47:38,3,government,0,2 816312869,0x0,US,US,0,31,25,
tcp-fin,0,0,0,0,,ATL-PAN-01, from-policy
Nov 15 08:47:57 10.1.0.2 1,2016/11/15 08:47: 57,001801015967,TRAFFIC,end, 1,2016/11/15
08:47:57,64.85. 77.9,50.232.155.145,64.85.77 .9,10.250.0.10,inbound-web-b rowsing,,,web-
browsing,vsys1 ,outside,dmz,ethernet1/4,eth ernet1/2,dell-secureworks,20 16/11/15
08:47:57,12863,1,58 815,80,58815,80,0x40001c,tcp ,allow,1216,801,415,9,2016/1 1/15
08:47:40,1,government,0 ,2816312840,0x0,US,US,0,6,3, tcp-rst-from-client,0,0,0,0, ,ATL-
PAN-01,from-policy
Nov 15 08:47:57 10.1.0.2 1,2016/ 11/15 08:47:57,001801015967, TRAFFIC,start,1,2016/11/15
0 8:47:57,98.18.199.154,50.232 .155.145,98.18.199.154,10.25 0.0.10,inbound-
web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-
secureworks,2016/11/15 08:47:57,36995,1,49698,80,4 9698,80,0x400000,tcp,allow,7
03,629,74,4,2016/11/15 08:47 :57,0,any,0,2816312877,0x0,U S,US,0,3,1,n/a,0,0,0,0,,ATL-
PAN-01,from-policy
Nov 15 08 :47:57 10.1.0.2 1,2016/11/15 08:47:57,001801015967,TRAFF
IC,start,1,2016/11/15 08:47: 57,12.167.43.50,50.232.155.1
45,12.167.43.50,10.250.0.10, inbound-web-browsing,,,web-b
rowsing,vsys1,outside,dmz,et hernet1/4,ethernet1/2,dell-s ecureworks,2016/11/15 08:47:
57,38395,1,52758,80,52758,80 ,0x400000,tcp,allow,1068,994 ,74,4,2016/11/15 08:47:56,0,
any,0,2816312872,0x0,US,US,0 ,3,1,n/a,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:47:57 10.1.0.2 1,2016/11/15 08:47 :57,001801015967,TRAFFIC,end ,1,2016/11/15
08:47:57,174.2 18.130.192,50.232.155.145,17 4.218.130.192,10.250.0.10,in bound-
web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec
ureworks,2016/11/15 08:47:57 ,241118,1,7177,80,7177,80,0x 40001c,tcp,allow,7572,1211,6
361,17,2016/11/15 08:47:39,2 ,government,0,2816312820,0x0 ,US,US,0,10,7,tcp-fin,0,0,0,
0,,ATL-PAN-01,from-policy
No v 15 08:47:55 10.1.0.2 1,201 6/11/15 08:47:55,00180101596 7,TRAFFIC,start,1,2016/11/15
08:47:55,192.35.47.1,50.232 .155.145,192.35.47.1,10.250. 0.10,inbound-web-browsing,,
web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0
8:47:55,45652,1,11988,80,119 88,80,0x400000,tcp,allow,471 ,405,66,4,2016/11/15 08:47:3
8,17,any,0,2816312730,0x0,US ,US,0,3,1,n/a,0,0,0,0,,ATL-P AN-01,from-policy
Nov 15 08: 47:56 10.1.0.2 1,2016/11/15 08:47:56,001801015967,TRAFFI C,end,1,2016/11/15
08:47:56, 64.85.77.11,50.232.155.145,6 4.85.77.11,10.250.0.10,inbou nd-web-
browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

works,2016/11/15 08:47:56,28 557,1,58544,80,58544,80,0x40 001c,tcp,allow,78498,11815,6
6683,126,2016/11/15 08:44:33 ,187,government,0,2816312762 ,0x0,US,US,0,69,57,tcp-rst-f
rom-client,0,0,0,0,,ATL-PAN- 01,from-policy
Nov 15 08:47: 56 10.1.0.2 1,2016/11/15 08: 47:56,001801015967,TRAFFIC,e nd,1,2016/11/15
08:47:56,152 .133.7.129,50.232.155.145,15 2.133.7.129,10.250.0.10,inbo und-web-
browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur
eworks,2016/11/15 08:47:56,4 2748,1,61739,80,61739,80,0x4 0001c,tcp,allow,4446,2747,16
99,12,2016/11/15 08:47:39,1, government,0,2816312743,0x0, US,US,0,7,5,tcp-rst-from-cli
ent,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:47:56 10.1 .0.2 1,2016/11/15 08:47:56,0 01801015967,TRAFFIC,end,1,20
16/11/15 08:47:56,152.133.7. 129,50.232.155.145,152.133.7 .129,10.250.0.10,inbound-web
-browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks,
2016/11/15 08:47:56,49357,1, 38211,80,38211,80,0x40001a,t cp,allow,4266,2627,1639,9,20
16/11/15 08:47:40,0,governme nt,0,2816312742,0x0,US,US,0, 5,4,tcp-rst-from-client,0,0,
0,0,,ATL-PAN-01,from-policy
Nov 15 08:47:55 10.1.0.2 1,2 016/11/15 08:47:55,001801015 967,TRAFFIC,end,1,2016/11/15
08:47:55,174.218.130.192,50 .232.155.145,174.218.130.192 ,10.250.0.10,inbound-
web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-
secureworks,2016 /11/15 08:47:55,51673,1,7172 ,80,7172,80,0x40001c,tcp,all
ow,37866,7927,29939,53,2016/ 11/15 08:47:39,0,government, 0,2816312682,0x0,US,US,0,29,
24,tcp-rst-from-client,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:47:55 10.1.0.2 1,20 16/11/15 08:47:55,0018010159 67,TRAFFIC,start,1,2016/11/1 5
08:47:55,192.35.47.1,50.23 2.155.145,192.35.47.1,10.250 .0.10,inbound-web-browsing,, ,web-
browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15
08:47:55,56285,1,41190,80,41 190,80,0x400000,tcp,allow,12 11,1145,66,4,2016/11/15 08:4
7:38,16,any,0,2816312691,0x0 ,US,US,0,3,1,n/a,0,0,0,0,,AT L-PAN-01,from-policy
Nov 15 08:47:55 10.1.0.2 1,2016/11/ 15 08:47:55,001801015967,TRA FFIC,end,1,2016/11/15
08:47: 55,98.159.233.10,50.232.155. 145,98.159.233.10,10.250.0.1 0,inbound-
web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -
secureworks,2016/11/15 08:4 7:55,53221,1,57061,80,57061, 80,0x40001a,tcp,allow,74855,
8669,66186,85,2016/11/15 08: 46:52,47,government,0,281631 2687,0x0,US,US,0,29,56,tcp-r
st-from-client,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :47:54 10.1.0.2 1,2016/11/15 08:47:54,001801015967,TRAFF IC,end,1,2016/11/15
08:47:54 ,192.35.47.1,50.232.155.145, 192.35.47.1,10.250.0.10,inbo und-web-browsing,,,web-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:47:54,4
6794,1,63959,80,63959,80,0x4 0001a,tcp,allow,2164,585,157 9,9,2016/11/15 08:47:38,0,go
vernment,0,2816312557,0x0,US ,US,0,6,3,tcp-rst-from-clien t,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:47:54 10.1.0 .2 1,2016/11/15 08:47:54,001 801015967,TRAFFIC,end,1,2016 /11/15
08:47:54,66.110.201.2 11,50.232.155.145,66.110.201 .211,10.250.0.10,inbound-
web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-
secureworks, 2016/11/15 08:47:54,38260,1, 62820,80,62820,80,0x40001a,t
cp,allow,17532,4525,13007,30 ,2016/11/15 08:47:21,17,gove rnment,0,2816312579,0x0,US,U
S,0,17,13,tcp-rst-from-clien t,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:47:53 10.1.0 .2 1,2016/11/15 08:47:53,001 801015967,TRAFFIC,end,1,2016 /11/15
08:47:53,64.85.77.2,5 0.232.155.145,64.85.77.2,10. 250.0.10,inbound-web-browsin g,,,web-
browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15
08:47:53,54728,1,60734,80 ,60734,80,0x40001c,tcp,allow ,37155,7370,29785,46,2016/11 /15
08:46:37,60,government,0 ,2816312499,0x0,US,US,0,23,2 3,tcp-fin,0,0,0,0,,ATL-PAN-0 1,from-
policy
Nov 15 08:47:5 3 10.1.0.2 1,2016/11/15 08:4 7:53,001801015967,TRAFFIC,en d,1,2016/11/15
08:47:53,64.8 5.97.219,50.232.155.145,64.8 5.97.219,10.250.0.10,inbound -web-
browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo
rks,2016/11/15 08:47:53,2590 3,1,56017,80,56017,80,0x4000 1c,tcp,allow,39528,8206,3132
2,56,2016/11/15 08:47:35,2,g overnment,0,2816312473,0x0,U S,US,0,31,25,tcp-rst-from-cl
ient,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:47:53 10. 1.0.2 1,2016/11/15 08:47:53, 001801015967,TRAFFIC,end,1,2 016/11/15
08:47:53,104.129.2 04.75,50.232.155.145,104.129 .204.75,10.250.0.10,inbound- web-
browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-securewor
ks,2016/11/15 08:47:53,25493 ,1,40443,80,40443,80,0x40001 c,tcp,allow,3410,1535,1875,1
7,2016/11/15 08:45:54,103,go vernment,0,2816312462,0x0,US ,US,0,10,7,tcp-fin,0,0,0,0,, ATL-
PAN-01,from-policy
Nov 1 5 08:47:53 10.1.0.2 1,2016/1 1/15 08:47:53,001801015967,T RAFFIC,end,1,2016/11/15
08:4 7:53,209.67.78.56,50.232.155 .145,209.67.78.56,10.250.0.1 0,inbound-
web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -
secureworks,2016/11/15 08:4 7:53,44463,1,60106,80,60106, 80,0x40001c,tcp,allow,99985,
13020,86965,140,2016/11/15 0 8:47:27,10,government,0,2816 312472,0x0,US,US,0,73,67,tcp -
rst-from-client,0,0,0,0,,AT L-PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:53 10.1.0.2 1,2016/11/ 15 08:47:53,001801015967,TRA FFIC,end,1,2016/11/15 08:47: 53,152.133.7.129,50.232.155. 145,152.133.7.129,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4 7:53,20193,1,61738,80,61738, 80,0x40001a,tcp,allow,84065, 16706,67359,90,2016/11/15 08 :47:29,8,government,0,281631 2471,0x0,US,US,0,35,55,tcp-r st-from-client,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :47:53 10.1.0.2 1,2016/11/15 08:47:53,001801015967,TRAFF IC,end,1,2016/11/15 08:47:53 ,104.129.204.75,50.232.155.1 45,104.129.204.75,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4 7:53,28484,1,2107,80,2107,80 ,0x40001c,tcp,allow,40095,58 49,34246,61,2016/11/15 08:45 :38,119,government,0,2816312 458,0x0,US,US,0,30,31,tcp-fi n,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:47:51 10.1.0 .2 1,2016/11/15 08:47:51,001 801015967,TRAFFIC,end,1,2016 /11/15 08:47:51,74.174.56.6, 50.232.155.145,74.174.56.6,1 0.250.0.10,inbound-web-brows ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15 08:47:51,46498,1,63722, 80,63722,80,0x40001c,tcp,all ow,69230,11169,58061,77,2016 /11/15 08:46:17,78,governmen t,0,2816312319,0x0,US,US,0,3 0,47,tcp-fin,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 7:51 10.1.0.2 1,2016/11/15 0 8:47:51,001801015967,TRAFFIC ,end,1,2016/11/15 08:47:51,4 7.32.70.122,50.232.155.145,4 7.32.70.122,10.250.0.10,inbo und-web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:47:51,3 4111,1,54718,80,54718,80,0x4 0001a,tcp,allow,65998,14187, 51811,73,2016/11/15 08:46:29 ,66,government,0,2816312286, 0x0,US,US,0,32,41,tcp-rst-fr om-client,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:47:5 1 10.1.0.2 1,2016/11/15 08:4 7:51,001801015967,TRAFFIC,en d,1,2016/11/15 08:47:51,64.8 5.97.245,50.232.155.145,64.8 5.97.245,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:47:51,3601 3,1,51931,80,51931,80,0x4000 1c,tcp,allow,88382,13903,744 79,129,2016/11/15 08:47:19,1 6,government,0,2816312280,0x 0,US,US,0,71,58,tcp-fin,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:47:51 10.1.0.2 1,2 016/11/15 08:47:51,001801015 967,TRAFFIC,end,1,2016/11/15 08:47:51,74.174.56.6,50.232 .155.145,74.174.56.6,10.250. 0.10,inbound-web-browsing,,, web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0 8:47:51,41351,1,48456,80,484 56,80,0x40001c,tcp,allow,561 8,3451,2167,16,2016/11/15

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

08 :46:17,78,government,0,28163 12292,0x0,US,US,0,10,6,tcp-f in,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08:47:51 10.1. 0.2 1,2016/11/15 08:47:51,00 1801015967,TRAFFIC,end,1,201 6/11/15 08:47:51,74.174.56.6 ,50.232.155.145,74.174.56.6, 10.250.0.10,inbound-web-brow sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/ 11/15 08:47:51,182728,1,1723 0,80,17230,80,0x40001c,tcp,a llow,1741,1350,391,9,2016/11 /15 08:46:17,78,government,0 ,2816312297,0x0,US,US,0,6,3, tcp-fin,0,0,0,0,,ATL-PAN-01, from-policy
Nov 15 08:47:50 10.1.0.2 1,2016/11/15 08:47: 50,001801015967,TRAFFIC,end, 1,2016/11/15 08:47:50,64.85. 77.2,50.232.155.145,64.85.77 .2,10.250.0.10,inbound-web-b rowsing,,,web-browsing,vsys1 ,outside,dmz,ethernet1/4,eth ernet1/2,dell-secureworks,20 16/11/15 08:47:50,243975,1,6 0691,80,60691,80,0x40001c,tc p,allow,51181,8588,42593,64, 2016/11/15 08:46:32,62,gover nment,0,2816312235,0x0,US,US ,0,31,33,tcp-fin,0,0,0,0,,AT L-PAN-01,from-policy
Nov 15 08:47:49 10.1.0.2 1,2016/11/ 15 08:47:49,001801015967,TRA FFIC,start,1,2016/11/15 08:4 7:49,64.85.97.149,50.232.155 .145,64.85.97.149,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4 7:49,33357,1,35568,80,35568, 80,0x400000,tcp,allow,600,52 6,74,4,2016/11/15 08:47:49,0 ,any,0,2816312205,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:47:4 9 10.1.0.2 1,2016/11/15 08:4 7:49,001801015967,TRAFFIC,en d,1,2016/11/15 08:47:49,209. 67.78.56,50.232.155.145,209. 67.78.56,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:47:49,1533 67,1,57386,80,57386,80,0x400 01c,tcp,allow,44152,3750,404 02,65,2016/11/15 08:47:08,25 ,government,0,2816312172,0x0 ,US,US,0,30,35,tcp-rst-from-server,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:47:48 1 0.1.0.2 1,2016/11/15 08:47:4 8,001801015967,TRAFFIC,end,1 ,2016/11/15 08:47:48,205.173 .105.205,50.232.155.145,205. 173.105.205,10.250.0.10,inbo und-web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:47:48,2 5288,1,63163,80,63163,80,0x4 0001a,tcp,allow,69659,7453,6 2206,80,2016/11/15 08:46:31, 61,government,0,2816312064,0 x0,US,US,0,30,50,tcp-rst-fro m-client,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:47:48 10.1.0.2 1,2016/11/15 08:47 :48,001801015967,TRAFFIC,end ,1,2016/11/15 08:47:48,205.1 73.105.205,50.232.155.145,20 5.173.105.205,10.250.0.10,in bound-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec
ureworks,2016/11/15 08:47:48 ,49318,1,58180,80,58180,80,0 x40001a,tcp,allow,4272,1180,
3092,12,2016/11/15 08:47:32, 0,government,0,2816312051,0x 0,US,US,0,7,5,tcp-rst-from-c
lient,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:47:46 10 .1.0.2 1,2016/11/15 08:47:46 ,001801015967,TRAFFIC,start, 1,2016/11/15
08:47:46,152.13 3.7.133,50.232.155.145,152.1 33.7.133,10.250.0.10,inbound -web-
browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo
rks,2016/11/15 08:47:46,3094 4,1,55017,80,55017,80,0x4000 00,tcp,allow,1606,1540,66,4,
2016/11/15 08:47:46,0,any,0, 2816311913,0x0,US,US,0,3,1,n /a,0,0,0,0,,ATL-PAN-01,from-
policy
Nov 15 08:47:47 10.1. 0.2 1,2016/11/15 08:47:47,00 1801015967,TRAFFIC,end,1,201
6/11/15 08:47:47,173.46.76.1 49,50.232.155.145,173.46.76. 149,10.250.0.10,inbound-web-
browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2
016/11/15 08:47:47,21779,1,1 9870,80,19870,80,0x40001c,tc p,allow,2388,711,1677,10,201
6/11/15 08:47:29,2,governmen t,0,2816311976,0x0,US,US,0,6 ,4,tcp-fin,0,0,0,0,,ATL-PAN-
01,from-policy
Nov 15 08:47: 47 10.1.0.2 1,2016/11/15 08: 47:47,001801015967,TRAFFIC,s
tart,1,2016/11/15 08:47:47,2 09.67.78.49,50.232.155.145,2 09.67.78.49,10.250.0.10,inbo
und-web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-
secur eworks,2016/11/15 08:47:47,6 4692,1,48780,80,48780,80,0x4
00000,tcp,allow,684,610,74,4 ,2016/11/15 08:47:46,0,any,0 ,2816311998,0x0,US,US,0,3,1, n/
a,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:47:46 10.1 .0.2 1,2016/11/15 08:47:46,0 01801015967,TRAFFIC,start,1, 2016/11/15
08:47:46,104.129. 204.75,50.232.155.145,104.12 9.204.75,10.250.0.10,inbound -web-
browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo
rks,2016/11/15 08:47:46,5685 1,1,21619,80,21619,80,0x4000 00,tcp,allow,1728,1654,74,4,
2016/11/15 08:47:46,0,any,0, 2816311909,0x0,US,US,0,3,1,n /a,0,0,0,0,,ATL-PAN-01,from-
policy
Nov 15 08:47:47 10.1. 0.2 1,2016/11/15 08:47:47,00 1801015967,TRAFFIC,end,1,201
6/11/15 08:47:47,64.85.77.10 ,50.232.155.145,64.85.77.10, 10.250.0.10,inbound-web-brow
sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/ 11/15
08:47:47,44233,1,43157 ,80,43157,80,0x40001c,tcp,al low,52337,10587,41750,73,201 6/11/15
08:46:49,42,governme nt,0,2816311973,0x0,US,US,0, 36,37,tcp-rst-from-server,0, 0,0,0,,ATL-
PAN-01,from-polic y

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:45 10.1.0.2 1 ,2016/11/15 08:47:45,0018010 15967,TRAFFIC,end,1,2016/11/
15 08:47:45,173.46.76.149,50 .232.155.145,173.46.76.149,1 0.250.0.10,inbound-web-brows
ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15
08:47:45,32035,1,19867, 80,19867,80,0x40001c,tcp,all ow,4783,773,4010,12,2016/11/ 15
08:47:28,1,government,0,2 816311736,0x0,US,US,0,7,5,tc p-fin,0,0,0,0,,ATL-PAN-01,fr om-
policy
Nov 15 08:47:45 10 .1.0.2 1,2016/11/15 08:47:45 ,001801015967,TRAFFIC,start, 1,2016/11/15
08:47:45,64.85. 77.12,50.232.155.145,64.85.7 7.12,10.250.0.10,inbound-web -browsing,,,web-
browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15
08:47:45,26171,1, 45901,80,45901,80,0x400000,t cp,allow,603,529,74,4,2016/1 1/15
08:47:45,0,any,0,281631 1780,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:47:46 10.1.0.2 1, 2016/11/15 08:47:46,00180101 5967,TRAFFIC,start,1,2016/11 /15
08:47:46,64.85.77.11,50. 232.155.145,64.85.77.11,10.2 50.0.10,inbound-web-browsing ,,,web-
browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5
08:47:46,34845,1,59330,80, 59330,80,0x400000,tcp,allow, 611,537,74,4,2016/11/15 08:4
7:45,0,any,0,2816311825,0x0, US,US,0,3,1,n/a,0,0,0,0,,ATL -PAN-01,from-policy
Nov 15 0 8:47:45 10.1.0.2 1,2016/11/1 5 08:47:45,001801015967,TRAF FIC,start,1,2016/11/15
08:47 :45,64.85.77.6,50.232.155.14 5,64.85.77.6,10.250.0.10,inb ound-web-browsing,,,web-
brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu reworks,2016/11/15 08:47:45,
45702,1,34378,80,34378,80,0x 400000,tcp,allow,693,619,74, 4,2016/11/15 08:47:44,0,any,
0,2816311654,0x0,US,US,0,3,1 ,n/a,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:47:44 10. 1.0.2 1,2016/11/15 08:47:44, 001801015967,TRAFFIC,start,1 ,2016/11/15
08:47:44,12.167. 43.50,50.232.155.145,12.167. 43.50,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4,
ethernet1/2,dell-secureworks ,2016/11/15 08:47:44,196682,
1,52757,80,52757,80,0x400000 ,tcp,allow,982,908,74,4,2016 /11/15 08:47:43,0,any,0,2816
311569,0x0,US,US,0,3,1,n/a,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:47:44 10.1.0.2 1,2016/11/15 08:47:44,001801 015967,TRAFFIC,end,1,2016/11 /15
08:47:44,173.46.76.149,5 0.232.155.145,173.46.76.149, 10.250.0.10,inbound-web-brow
sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/ 11/15
08:47:44,52619,1,19865 ,80,19865,80,0x40001c,tcp,al low,4849,839,4010,13,2016/11 /15
08:47:28,0,government,0, 2816311585,0x0,US,US,0,8,5,t cp-fin,0,0,0,0,,ATL-PAN-01,f rom-
policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:44 1 0.1.0.2 1,2016/11/15 08:47:4 4,001801015967,TRAFFIC,end,1 ,2016/11/15 08:47:44,66.192. 63.2,50.232.155.145,66.192.6 3.2,10.250.0.10,inbound-web- browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2 016/11/15 08:47:44,34026,1,6 4531,80,64531,80,0x40001c,tc p,allow,75940,16870,59070,67 ,2016/11/15 08:46:22,66,gove rnment,0,2816311602,0x0,US,U S,0,24,43,tcp-fin,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:47:44 10.1.0.2 1,2016/11 /15 08:47:44,001801015967,TR AFFIC,end,1,2016/11/15 08:47 :44,207.99.81.78,50.232.155. 145,207.99.81.78,10.250.0.10 ,inbound-web-browsing,,,web- browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell-secureworks,2016/11/15 08:47 :44,28540,1,2623,80,2623,80, 0x40001a,tcp,allow,84700,145 67,70133,93,2016/11/15 08:46 :30,58,government,0,28163116 13,0x0,US,US,0,33,60,tcp-rst - from-client,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 7:44 10.1.0.2 1,2016/11/15 0 8:47:44,001801015967,TRAFFIC ,start,1,2016/11/15 08:47:44 ,66.194.234.196,50.232.155.1 45,66.194.234.196,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell - secureworks,2016/11/15 08:4 7:44,50315,1,38772,80,38772, 80,0x400000,tcp,allow,655,58 9,66,4,2016/11/15 08:47:43,1 ,any,0,2816311633,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:47:4 4 10.1.0.2 1,2016/11/15 08:4 7:44,001801015967,TRAFFIC,st art,1,2016/11/15 08:47:44,66 .194.234.196,50.232.155.145, 66.194.234.196,10.250.0.10,i nbound-web-browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15 08:47:4 4,50256,1,40224,80,40224,80, 0x400000,tcp,allow,559,493,6 6,4,2016/11/15 08:47:43,0,an y,0,2816311622,0x0,US,US,0,3 ,1,n/a,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:47:44 1 0.1.0.2 1,2016/11/15 08:47:4 4,001801015967,TRAFFIC,end,1 ,2016/11/15 08:47:44,152.133 .7.129,50.232.155.145,152.13 3.7.129,10.250.0.10,inbound-web-browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-securewor ks,2016/11/15 08:47:44,52014 ,1,61007,80,61007,80,0x40001 a,tcp,allow,17045,5711,11334 ,23,2016/11/15 08:47:23,5,go vernment,0,2816311614,0x0,US ,US,0,12,11,tcp-rst-from-cli ent,0,0,0,0,,ATL-PAN-01,from - policy
Nov 15 08:47:44 10.1 .0.2 1,2016/11/15 08:47:44,0 01801015967,TRAFFIC,end,1,20 16/11/15 08:47:44,12.167.43. 50,50.232.155.145,12.167.43. 50,10.250.0.10,inbound-web-b rowsing,,,web-browsing,vsys1 ,outside,dmz,ethernet1/4,eth ernet1/2,dell-secureworks,20

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

16/11/15 08:47:44,31435,1,52 746,80,52746,80,0x40001c,tcp ,allow,31487,2030,29457,42,2
016/11/15 08:47:27,1,governm ent,0,2816311615,0x0,US,US,0 ,20,22,tcp-fin,0,0,0,0,,ATL-
PAN-01,from-policy
Nov 15 08 :47:44 10.1.0.2 1,2016/11/15 08:47:44,001801015967,TRAFF IC,start,1,2016/11/15
08:47: 44,66.194.234.196,50.232.155 .145,66.194.234.196,10.250.0 .10,inbound-
web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-
secureworks,2016/11/15 08 :47:44,38033,1,41472,80,4147 2,80,0x400000,tcp,allow,670,
604,66,4,2016/11/15 08:47:44 ,0,any,0,2816311639,0x0,US,U S,0,3,1,n/a,0,0,0,0,,ATL-PAN
-01,from-policy
Nov 15 08:47 :43 10.1.0.2 1,2016/11/15 08 :47:43,001801015967,TRAFFIC, end,1,2016/11/15
08:47:43,47 .32.70.122,50.232.155.145,47 .32.70.122,10.250.0.10,inbou nd-web-
browsing,,,incomplete ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo
rks,2016/11/15 08:47:43,4613 6,1,54725,80,54725,80,0x4000 1b,tcp,allow,312,186,126,5,2
016/11/15 08:47:02,25,any,0, 2816311511,0x0,US,US,0,3,2,t cp-rst-from-server,0,0,0,0,, ATL-
PAN-01,from-policy
Nov 1 5 08:47:43 10.1.0.2 1,2016/1 1/15 08:47:43,001801015967,T RAFFIC,start,1,2016/11/15
08 :47:43,205.173.105.205,50.23 2.155.145,205.173.105.205,10 .250.0.10,inbound-web-browsi
ng,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15
08:47:43,24150,1,41564,8 0,41564,80,0x400000,tcp,allo w,629,563,66,4,2016/11/15
08 :47:32,11,any,0,2816311532,0 x0,US,US,0,3,1,n/a,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:47:43 10.1.0.2 1,2016/1 1/15 08:47:43,001801015967,T RAFFIC,start,1,2016/11/15
08 :47:43,205.173.105.205,50.23 2.155.145,205.173.105.205,10 .250.0.10,inbound-web-browsi
ng,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15
08:47:43,48824,1,46851,8 0,46851,80,0x400000,tcp,allo w,629,563,66,4,2016/11/15
08 :47:43,0,any,0,2816311533,0x 0,US,US,0,3,1,n/a,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:47:43 10.1.0.2 1,2016/11 /15 08:47:43,001801015967,TR AFFIC,end,1,2016/11/15
08:47 :43,209.67.78.57,50.232.155. 145,209.67.78.57,10.250.0.10 ,inbound-
web-browsing,,,web- browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell-
secureworks,2016/11/15 08:47 :43,30852,1,51081,80,51081,8 0,0x40001c,tcp,allow,20481,1
970,18511,35,2016/11/15 08:4 7:21,6,government,0,28163114 97,0x0,US,US,0,19,16,tcp-
fin ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:47:43 10.1.0. 2 1,2016/11/15 08:47:43,0018 01015967,TRAFFIC,start,1,201
6/11/15 08:47:43,209.67.78.5 0,50.232.155.145,209.67.78.5 0,10.250.0.10,inbound-web-br
owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

6/11/15 08:47:43,11932,1,337 75,80,33775,80,0x400000,tcp, allow,650,576,74,4,2016/11/1 5
08:47:42,0,any,0,281631148 9,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:47:43 10.1.0.2 1,201 6/11/15 08:47:43,00180101596 7,TRAFFIC,end,1,2016/11/15
0 8:47:43,64.85.77.12,50.232.1 55.145,64.85.77.12,10.250.0. 10,inbound-web-browsing,,,in
complete,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell- secureworks,2016/11/15
08:47 :43,59525,1,50997,80,50997,8 0,0x40001b,tcp,allow,340,206 ,134,5,2016/11/15
08:47:27,0 ,any,0,2816311504,0x0,US,US, 0,3,2,tcp-rst-from-server,0, 0,0,0,,ATL-PAN-01,from-
polic y
Nov 15 08:47:43 10.1.0.2 1 ,2016/11/15 08:47:43,0018010 15967,TRAFFIC,end,1,2016/11/
15 08:47:43,47.32.70.122,50. 232.155.145,47.32.70.122,10. 250.0.10,inbound-web-browsin
g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15
08:47:43,32993,1,54724,80 ,54724,80,0x40001a,tcp,allow ,16760,3949,12811,23,2016/11 /15
08:47:02,25,government,0 ,2816311512,0x0,US,US,0,11,1 2,tcp-rst-from-client,0,0,0, 0,,ATL-
PAN-01,from-policy
No v 15 08:47:42 10.1.0.2 1,201 6/11/15 08:47:42,00180101596 7,TRAFFIC,end,1,2016/11/15
0 8:47:42,98.159.233.10,50.232 .155.145,98.159.233.10,10.25 0.0.10,inbound-
web-browsing, ,,incomplete,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d
ell-secureworks,2016/11/15 0 8:47:42,49394,1,57088,80,570
88,80,0x40001b,tcp,allow,344 ,210,134,5,2016/11/15 08:47:
21,5,any,0,2816311437,0x0,US ,US,0,3,2,tcp-rst-from-serve r,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:47:42 10.1.0 .2 1,2016/11/15 08:47:42,001 801015967,TRAFFIC,start,1,20
16/11/15 08:47:42,108.66.253 .68,50.232.155.145,108.66.25 3.68,10.250.0.10,inbound-web
-browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks,
2016/11/15 08:47:42,44282,1, 60785,80,60785,80,0x400000,t cp,allow,790,724,66,4,2016/1
1/15 08:47:41,0,any,0,281631 1458,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:47:42 10.1.0.2 1, 2016/11/15 08:47:42,00180101 5967,TRAFFIC,start,1,2016/11 /15
08:47:42,68.156.159.10,5 0.232.155.145,68.156.159.10, 10.250.0.10,inbound-web-brow
sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/
11/15 08:47:42,56156,1,35074 ,80,35074,80,0x400000,tcp,al low,699,633,66,4,2016/11/15
08:47:42,0,any,0,2816311466, 0x0,US,US,0,3,1,n/a,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:47:42 10.1.0.2 1,2016/ 11/15 08:47:42,001801015967, TRAFFIC,start,1,2016/11/15
0 8:47:42,209.60.129.66,50.232 .155.145,209.60.129.66,10.25 0.0.10,inbound-
web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-
secureworks,2016/11/15 08:47:42,15142,1,45986,80,4 5986,80,0x400000,tcp,allow,6

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

81,615,66,4,2016/11/15 08:47 :42,0,any,0,2816311468,0x0,U S,US,0,3,1,n/a,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08 :47:42 10.1.0.2 1,2016/11/15 08:47:42,001801015967,TRAFF IC,start,1,2016/11/15 08:47: 42,209.60.129.66,50.232.155. 145,209.60.129.66,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell - secureworks,2016/11/15 08:4 7:42,40824,1,54924,80,54924, 80,0x400000,tcp,allow,675,60 9,66,4,2016/11/15 08:47:42,0 ,any,0,2816311474,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:47:4 2 10.1.0.2 1,2016/11/15 08:4 7:42,001801015967,TRAFFIC,st art,1,2016/11/15 08:47:42,68 .156.159.10,50.232.155.145,6 8.156.159.10,10.250.0.10,inb ound-web-browsing,,,web-brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu reworks,2016/11/15 08:47:42, 44888,1,42595,80,42595,80,0x 400000,tcp,allow,700,634,66, 4,2016/11/15 08:47:42,0,any, 0,2816311487,0x0,US,US,0,3,1 ,n/a,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:47:41 10. 1.0.2 1,2016/11/15 08:47:41, 001801015967,TRAFFIC,start,1 ,2016/11/15 08:47:41,64.85.9 7.175,50.232.155.145,64.85.9 7.175,10.250.0.10,inbound-we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-secureworks ,2016/11/15 08:47:41,46830,1 ,51175,80,51175,80,0x400000, tcp,allow,684,610,74,4,2016/ 11/15 08:47:40,1,any,0,28163 11358,0x0,US,US,0,3,1,n/a,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:47:41 10.1.0.2 1 ,2016/11/15 08:47:41,0018010 15967,TRAFFIC,start,1,2016/1 1/15 08:47:41,64.85.77.9,50. 232.155.145,64.85.77.9,10.25 0.0.10,inbound-web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15 08:47:41,12863,1,58815,80,5 8815,80,0x400000,tcp,allow,6 89,615,74,4,2016/11/15 08:47 :40,0,any,0,2816311355,0x0,U S,US,0,3,1,n/a,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :47:40 10.1.0.2 1,2016/11/15 08:47:40,001801015967,TRAFF IC,start,1,2016/11/15 08:47: 40,174.218.130.192,50.232.15 5.145,174.218.130.192,10.250 .0.10,inbound-web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15 08:47:40,241118,1,7177,80,71 77,80,0x400000,tcp,allow,823 ,749,74,4,2016/11/15 08:47:3 9,0,any,0,2816311291,0x0,US, US,0,3,1,n/a,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 7:39 10.1.0.2 1,2016/11/15 0 8:47:39,001801015967,TRAFFIC ,start,1,2016/11/15 08:47:39 ,64.85.77.7,50.232.155.145,6 4.85.77.7,10.250.0.10,inboun d-web-browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew orks,2016/11/15

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

08:47:39,385 32,1,56586,80,56586,80,0x400 000,tcp,allow,703,629,74,4,2 016/11/15
08:47:39,0,any,0,2 816311254,0x0,US,US,0,3,1,n/ a,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:47:40 10.1.0 .2 1,2016/11/15 08:47:40,001 801015967,TRAFFIC,start,1,20
16/11/15 08:47:40,152.133.7. 129,50.232.155.145,152.133.7 .129,10.250.0.10,inbound-
web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-
secureworks, 2016/11/15 08:47:40,42748,1, 61739,80,61739,80,0x400000,t
cp,allow,1606,1540,66,4,2016 /11/15 08:47:39,1,any,0,2816 311299,0x0,US,US,0,3,1,n/
a,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:47:39 10.1.0.2 1,2016/11/15 08:47:39,001801 015967,TRAFFIC,start,1,2016/
11/15 08:47:39,152.133.7.129 ,50.232.155.145,152.133.7.12 9,10.250.0.10,inbound-web-
br owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201
6/11/15 08:47:39,259243,1,61 740,80,61740,80,0x400000,tcp ,allow,1606,1540,66,4,2016/1
1/15 08:47:39,0,any,0,281631 1266,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:47:40 10.1.0.2 1, 2016/11/15 08:47:40,00180101 5967,TRAFFIC,start,1,2016/11 /15
08:47:40,152.133.7.129,5 0.232.155.145,152.133.7.129, 10.250.0.10,inbound-web-brow
sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/
11/15 08:47:40,49357,1,38211 ,80,38211,80,0x400000,tcp,al low,1606,1540,66,4,2016/11/1 5
08:47:40,0,any,0,281631130 0,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:47:39 10.1.0.2 1,201 6/11/15 08:47:39,00180101596 7,TRAFFIC,start,1,2016/11/15
08:47:39,174.218.130.192,50 .232.155.145,174.218.130.192 ,10.250.0.10,inbound-
web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-
secureworks,2016 /11/15 08:47:39,51673,1,7172 ,80,7172,80,0x400000,tcp,all
ow,1656,1582,74,4,2016/11/15 08:47:39,0,any,0,2816311265 ,0x0,US,US,0,3,1,n/
a,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:47:38 10.1.0.2 1,2016 /11/15 08:47:38,001801015967 ,TRAFFIC,start,1,2016/11/15
08:47:38,192.35.47.1,50.232. 155.145,192.35.47.1,10.250.0 .10,inbound-web-browsing,,,w
eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15
08 :47:38,27697,1,2880,80,2880, 80,0x400000,tcp,allow,1144,1 078,66,4,2016/11/15
08:47:38 ,0,any,0,2816311174,0x0,US,U S,0,3,1,n/a,0,0,0,0,,ATL-PAN -01,from-policy
Nov 15 08:47 :39 10.1.0.2 1,2016/11/15 08 :47:39,001801015967,TRAFFIC, end,1,2016/11/15
08:47:39,15 2.133.7.129,50.232.155.145,1 52.133.7.129,10.250.0.10,inb ound-
web-browsing,,,web-brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu
reworks,2016/11/15 08:47:39, 52489,1,33536,80,33536,80,0x 40001a,tcp,allow,4386,2747,1

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

639,11,2016/11/15 08:47:23,0 ,government,0,2816311215,0x0 ,US,US,0,7,4,tcp-rst-from-cl
ient,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:47:39 10. 1.0.2 1,2016/11/15 08:47:39, 001801015967,TRAFFIC,end,1,2
016/11/15 08:47:39,98.159.23 3.10,50.232.155.145,98.159.2 33.10,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4,
ethernet1/2,dell-secureworks ,2016/11/15 08:47:39,254121,
1,57058,80,57058,80,0x40001a ,tcp,allow,80470,10683,69787 ,92,2016/11/15 08:46:52,31,g
overnment,0,2816311234,0x0,U S,US,0,32,60,tcp-rst-from-cl ient,0,0,0,0,,ATL-PAN-01,fro m-
policy
Nov 15 08:47:38 10. 1.0.2 1,2016/11/15 08:47:38, 001801015967,TRAFFIC,start,1 ,2016/11/15
08:47:38,64.85.9 7.251,50.232.155.145,64.85.9 7.251,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-
secureworks ,2016/11/15 08:47:38,11964,1 ,56654,80,56654,80,0x400000,
tcp,allow,603,529,74,4,2016/ 11/15 08:47:38,0,any,0,28163 11195,0x0,US,US,0,3,1,n/a,0,
0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:47:38 10.1.0.2 1 ,2016/11/15 08:47:38,0018010 15967,TRAFFIC,start,1,2016/1
1/15 08:47:38,66.110.201.211 ,50.232.155.145,66.110.201.2 11,10.250.0.10,inbound-web-
b rowsing,,,web-browsing,vsys1 ,outside,dmz,ethernet1/4,eth ernet1/2,dell-secureworks,20
16/11/15 08:47:38,46878,1,62 821,80,62821,80,0x400000,tcp ,allow,1728,1654,74,4,2016/1
1/15 08:47:21,17,any,0,28163 11172,0x0,US,US,0,3,1,n/a,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:47:38 10.1.0.2 1 ,2016/11/15 08:47:38,0018010 15967,TRAFFIC,start,1,2016/1
1/15 08:47:38,192.35.47.1,50 .232.155.145,192.35.47.1,10. 250.0.10,inbound-web-browsin
g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/
15 08:47:38,46794,1,63959,80 ,63959,80,0x400000,tcp,allow ,471,405,66,4,2016/11/15 08:
47:38,0,any,0,2816311197,0x0 ,US,US,0,3,1,n/a,0,0,0,0,,AT L-PAN-01,from-policy
Nov 15 08:47:39 10.1.0.2 1,2016/11/ 15 08:47:39,001801015967,TRA FFIC,end,1,2016/11/15
08:47: 39,152.133.7.129,50.232.155. 145,152.133.7.129,10.250.0.1 0,inbound-
web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -
secureworks,2016/11/15 08:4 7:39,48461,1,11160,80,11160, 80,0x40001a,tcp,allow,4266,2
627,1639,9,2016/11/15 08:47: 23,0,government,0,2816311226 ,0x0,US,US,0,5,4,tcp-rst-fro m-
client,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:47:38 10.1.0.2 1,2016/11/15 08:47 :38,001801015967,TRAFFIC,sta rt,1,2016/11/15
08:47:38,192 .35.47.1,50.232.155.145,192. 35.47.1,10.250.0.10,inbound- web-browsing,,,web-
browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-securewor ks,2016/11/15

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

08:47:38,54904 ,1,27330,80,27330,80,0x40000 0,tcp,allow,1118,1052,66,4,2 016/11/15
08:47:38,0,any,0,2 816311171,0x0,US,US,0,3,1,n/ a,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:47:38 10.1.0 .2 1,2016/11/15 08:47:38,001 801015967,TRAFFIC,start,1,20
16/11/15 08:47:38,66.110.201 .211,50.232.155.145,66.110.2 01.211,10.250.0.10,inbound-
w eb-browsing,,,web-browsing,v sys1,outside,dmz,ethernet1/4 ,ethernet1/2,dell-securework
s,2016/11/15 08:47:38,38260, 1,62820,80,62820,80,0x400000 ,tcp,allow,1728,1654,74,4,20
16/11/15 08:47:21,16,any,0,2 816311155,0x0,US,US,0,3,1,n/ a,0,0,0,0,,ATL-PAN-01,from-p
olicy
Nov 15 08:47:38 10.1.0 .2 1,2016/11/15 08:47:38,001 801015967,TRAFFIC,start,1,20 16/11/15
08:47:38,192.35.47. 1,50.232.155.145,192.35.47.1 ,10.250.0.10,inbound-web-bro wsing,,,web-
browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15
08:47:38,51161,1,6044 9,80,60449,80,0x400000,tcp,a llow,1069,1003,66,4,2016/11/ 15
08:47:38,0,any,0,28163111 68,0x0,US,US,0,3,1,n/a,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:47:38 10.1.0.2 1,20 16/11/15 08:47:38,0018010159 67,TRAFFIC,start,1,2016/11/1
5 08:47:38,209.67.78.57,50.2 32.155.145,209.67.78.57,10.2 50.0.10,inbound-
web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-
secureworks,2016/11/1 5 08:47:38,37059,1,40253,80, 40253,80,0x400000,tcp,allow,
600,526,74,4,2016/11/15 08:4 7:37,1,any,0,2816311162,0x0, US,US,0,3,1,n/a,0,0,0,0,,ATL -
PAN-01,from-policy
Nov 15 0 8:47:37 10.1.0.2 1,2016/11/1 5 08:47:37,001801015967,TRAF
FIC,end,1,2016/11/15 08:47:3 7,74.183.101.197,50.232.155.
145,74.183.101.197,10.250.0. 10,inbound-web-browsing,,,we b-
browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08:
47:37,46295,1,53630,80,53630 ,80,0x40001c,tcp,allow,19370 ,4388,14982,40,2016/11/15
08 :46:51,30,government,0,28163 11041,0x0,US,US,0,26,14,tcp- fin,0,0,0,0,,ATL-PAN-01,from
-policy
Nov 15 08:47:37 10.1 .0.2 1,2016/11/15 08:47:37,0 01801015967,TRAFFIC,end,1,20
16/11/15 08:47:37,205.173.10 5.205,50.232.155.145,205.173 .105.205,10.250.0.10,inbound
-web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo
rks,2016/11/15 08:47:37,2102 5,1,58177,80,58177,80,0x4000 1a,tcp,allow,42241,8690,3355
1,51,2016/11/15 08:46:31,50, government,0,2816311049,0x0, US,US,0,22,29,tcp-rst-from-c
lient,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:47:37 10 .1.0.2 1,2016/11/15 08:47:37 ,001801015967,TRAFFIC,end,1, 2016/11/15
08:47:37,66.110.2 01.211,50.232.155.145,66.110 .201.211,10.250.0.10,inbound -web-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo
rks,2016/11/15 08:47:37,6359 2,1,62817,80,62817,80,0x4000 1a,tcp,allow,4254,1238,3016,
10,2016/11/15 08:47:20,1,gov ernment,0,2816311048,0x0,US, US,0,7,3,tcp-rst-from-
client ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:47:37 10.1.0. 2 1,2016/11/15 08:47:37,0018 01015967,TRAFFIC,end,1,2016/
11/15 08:47:37,12.48.151.106 ,50.232.155.145,12.48.151.10 6,10.250.0.10,inbound-web-
br owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201
6/11/15 08:47:37,50174,1,197 5,80,1975,80,0x40001a,tcp,al low,2328,749,1579,8,2016/11/
15 08:46:14,67,government,0, 2816311019,0x0,US,US,0,5,3,t cp-rst-from-client,0,0,0,0,, ATL-
PAN-01,from-policy
Nov 1 5 08:47:37 10.1.0.2 1,2016/1 1/15 08:47:37,001801015967,T RAFFIC,end,1,2016/11/15
08:4 7:37,152.133.7.129,50.232.15 5.145,152.133.7.129,10.250.0 .10,inbound-
web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-
secureworks,2016/11/15 08 :47:37,41230,1,24538,80,2453 8,80,0x40001a,tcp,allow,8400
3,16646,67357,89,2016/11/15 08:47:13,8,government,0,2816 311044,0x0,US,US,0,34,55,tcp -
rst-from-client,0,0,0,0,,AT L-PAN-01,from-policy
Nov 15 08:47:37 10.1.0.2 1,2016/11/ 15 08:47:37,001801015967,TRA FFIC,end,1,2016/11/15
08:47: 37,12.48.151.106,50.232.155. 145,12.48.151.106,10.250.0.1 0,inbound-
web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -
secureworks,2016/11/15 08:4 7:37,58830,1,64516,80,64516, 80,0x40001a,tcp,allow,12408,
1108,11300,21,2016/11/15 08: 46:14,67,government,0,281631 1039,0x0,US,US,0,11,10,tcp-r
st-from-client,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :47:36 10.1.0.2 1,2016/11/15 08:47:36,001801015967,TRAFF IC,end,1,2016/11/15
08:47:36 ,70.133.222.130,50.232.155.1 45,70.133.222.130,10.250.0.1 0,inbound-
web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -
secureworks,2016/11/15 08:4 7:36,45867,1,61086,80,61086, 80,0x40001c,tcp,allow,22448,
4656,17792,42,2016/11/15 08: 46:20,60,government,0,281631 0897,0x0,US,US,0,28,14,tcp-f
in,0,0,0,0,,ATL-PAN-01,from- policy
Nov 15 08:47:36 10.1. 0.2 1,2016/11/15 08:47:36,00 1801015967,TRAFFIC,start,1,2
016/11/15 08:47:36,64.85.97. 219,50.232.155.145,64.85.97. 219,10.250.0.10,inbound-web-
browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2
016/11/15 08:47:36,25903,1,5 6017,80,56017,80,0x400000,tc p,allow,684,610,74,4,2016/11 /15
08:47:35,0,any,0,2816310 884,0x0,US,US,0,3,1,n/a,0,0, 0,0,,ATL-PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:36 10.1.0.2 1,2 016/11/15 08:47:36,001801015 967,TRAFFIC,end,1,2016/11/15 08:47:36,66.110.201.211,50. 232.155.145,66.110.201.211,1 0.250.0.10,inbound-web-brows ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15 08:47:36,26783,1,62811, 80,62811,80,0x40001a,tcp,all ow,8743,4124,4619,17,2016/11 /15 08:46:38,42,government,0 ,2816310904,0x0,US,US,0,11,6 ,tcp-rst-from-client,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:47:35 10.1.0.2 1,2016 /11/15 08:47:35,001801015967 ,TRAFFIC,end,1,2016/11/15 08 :47:35,64.85.97.203,50.232.1 55.145,64.85.97.203,10.250.0 .10,inbound-web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15 08 :47:35,48057,1,46679,80,4667 9,80,0x40001c,tcp,allow,1183 10,15938,102372,168,2016/11/ 15 08:46:50,29,government,0, 2816310812,0x0,US,US,0,89,79 ,tcp-rst-from-client,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:47:35 10.1.0.2 1,2016 /11/15 08:47:35,001801015967 ,TRAFFIC,end,1,2016/11/15 08 :47:35,64.85.77.14,50.232.15 5.145,64.85.77.14,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4 7:35,36790,1,33344,80,33344, 80,0x40001c,tcp,allow,7828,2 724,5104,21,2016/11/15 08:46 :05,74,government,0,28163108 15,0x0,US,US,0,14,7,tcp-fin, 0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:47:35 10.1.0.2 1,2016/11/15 08:47:35,00180 1015967,TRAFFIC,end,1,2016/1 1/15 08:47:35,171.159.64.10, 50.232.155.145,171.159.64.10 ,10.250.0.10,inbound-web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:47:35,261048,1,100 02,80,10002,80,0x40001c,tcp, allow,61190,9291,51899,74,20 16/11/15 08:46:55,24,governm ent,0,2816310833,0x0,US,US,0 ,33,41,tcp-fin,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :47:33 10.1.0.2 1,2016/11/15 08:47:33,001801015967,TRAFF IC,end,1,2016/11/15 08:47:33 ,64.85.77.12,50.232.155.145, 64.85.77.12,10.250.0.10,inbo und-web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:47:33,4 5270,1,52197,80,52197,80,0x4 0001c,tcp,allow,3151,1265,18 86,12,2016/11/15 08:46:16,61 ,government,0,2816310676,0x0 ,US,US,0,8,4,tcp-fin,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:47:33 10.1.0.2 1,2016 /11/15 08:47:33,001801015967 ,TRAFFIC,start,1,2016/11/15 08:47:33,205.173.105.205,50. 232.155.145,205.173.105.205, 10.250.0.10,inbound-web-brow sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

11/15 08:47:33,49318,1,58180 ,80,58180,80,0x400000,tcp,al low,629,563,66,4,2016/11/15 08:47:32,0,any,0,2816310628, 0x0,US,US,0,3,1,n/a,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:47:31 10.1.0.2 1,2016/ 11/15 08:47:31,001801015967, TRAFFIC,end,1,2016/11/15 08: 47:31,152.133.7.133,50.232.1 55.145,152.133.7.133,10.250. 0.10,inbound-web-browsing,,, web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0 8:47:31,19113,1,12667,80,126 67,80,0x40001a,tcp,allow,797 0,4170,3800,15,2016/11/15 08 :46:53,22,government,0,28163 10467,0x0,US,US,0,8,7,tcp-rs t-from-client,0,0,0,0,,ATL-P AN-01,from-policy
Nov 15 08: 47:31 10.1.0.2 1,2016/11/15 08:47:31,001801015967,TRAFFI C,end,1,2016/11/15 08:47:31, 66.192.63.2,50.232.155.145,6 6.192.63.2,10.250.0.10,inbou nd-web-browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure works,2016/11/15 08:47:31,25 6012,1,30379,80,30379,80,0x4 0001c,tcp,allow,75915,16946, 58969,69,2016/11/15 08:46:08 ,67,government,0,2816310469, 0x0,US,US,0,25,44,tcp-fin,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:47:31 10.1.0.2 1 ,2016/11/15 08:47:31,0018010 15967,TRAFFIC,end,1,2016/11/ 15 08:47:31,209.67.78.55,50. 232.155.145,209.67.78.55,10. 250.0.10,inbound-web-browsin g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15 08:47:31,37585,1,58152,80 ,58152,80,0x40001c,tcp,allow ,18231,4968,13263,41,2016/11 /15 08:47:08,7,government,0, 2816310470,0x0,US,US,0,26,15 ,tcp-fin,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:47:31 10.1.0.2 1,2016/11/15 08:47 :31,001801015967,TRAFFIC,end ,1,2016/11/15 08:47:31,205.1 73.105.205,50.232.155.145,20 5.173.105.205,10.250.0.10,in bound-web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec ureworks,2016/11/15 08:47:31 ,40026,1,65288,80,65288,80,0 x40001a,tcp,allow,7118,1925, 5193,16,2016/11/15 08:46:31, 44,government,0,2816310491,0 x0,US,US,0,9,7,tcp-rst-from-client,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:47:32 1 0.1.0.2 1,2016/11/15 08:47:3 2,001801015967,TRAFFIC,end,1 ,2016/11/15 08:47:32,64.85.7 7.6,50.232.155.145,64.85.77. 6,10.250.0.10,inbound-web-br owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201 6/11/15 08:47:32,27007,1,339 19,80,33919,80,0x40001c,tcp, allow,14441,2774,11667,28,20 16/11/15 08:47:10,6,governme nt,0,2816310549,0x0,US,US,0, 16,12,tcp-rst-from-client,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:47:30 10.1.0.2 1 ,2016/11/15 08:47:30,0018010 15967,TRAFFIC,start,1,2016/1 1/15 08:47:30,152.133.7.129, 50.232.155.145,152.133.7.129 ,10.250.0.10,inbound-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:47:30,33745,1,6173 7,80,61737,80,0x400000,tcp,a llow,1606,1540,66,4,2016/11/ 15 08:47:29,0,any,0,28163104 21,0x0,US,US,0,3,1,n/a,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:47:30 10.1.0.2 1,20 16/11/15 08:47:30,0018010159 67,TRAFFIC,end,1,2016/11/15 08:47:30,96.91.139.57,50.232 .155.145,96.91.139.57,10.250 .0.10,inbound-web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15 08:47:30,47457,1,50999,80,50 999,80,0x40001b,tcp,allow,10 5136,14541,90595,109,2016/11 /15 08:43:06,248,government, 0,2816310370,0x0,US,US,0,35, 74,tcp-rst-from-server,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:47:29 10.1.0.2 1,20 16/11/15 08:47:29,0018010159 67,TRAFFIC,end,1,2016/11/15 08:47:29,152.133.7.129,50.23 2.155.145,152.133.7.129,10.2 50.0.10,inbound-web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5 08:47:29,12205,1,54312,80, 54312,80,0x40001a,tcp,allow, 4221,2582,1639,9,2016/11/15 08:47:13,0,government,0,2816 310294,0x0,US,US,0,5,4,tcp-r st-from-client,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :47:30 10.1.0.2 1,2016/11/15 08:47:30,001801015967,TRAFF IC,start,1,2016/11/15 08:47: 30,152.133.7.129,50.232.155. 145,152.133.7.129,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4 7:30,20193,1,61738,80,61738, 80,0x400000,tcp,allow,1606,1 540,66,4,2016/11/15 08:47:29 ,0,any,0,2816310354,0x0,US,U S,0,3,1,n/a,0,0,0,0,,ATL-PAN -01,from-policy
Nov 15 08:47 :29 10.1.0.2 1,2016/11/15 08 :47:29,001801015967,TRAFFIC, start,1,2016/11/15 08:47:29, 173.46.76.149,50.232.155.145 ,173.46.76.149,10.250.0.10,i nbound-web-browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15 08:47:2 9,21779,1,19870,80,19870,80, 0x400000,tcp,allow,587,513,7 4,4,2016/11/15 08:47:29,0,an y,0,2816310313,0x0,US,US,0,3 ,1,n/a,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:47:29 1 0.1.0.2 1,2016/11/15 08:47:2 9,001801015967,TRAFFIC,end,1 ,2016/11/15 08:47:29,64.179. 192.42,50.232.155.145,64.179 .192.42,10.250.0.10,inbound- web-browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-securewor ks,2016/11/15 08:47:29,36698 ,1,57922,80,57922,80,0x40001 a,tcp,allow,48297,10298,3799 9,65,2016/11/15 08:47:01,12, government,0,2816310281,0x0, US,US,0,35,30,tcp-rst-from-c lient,0,0,0,0,,ATL-PAN-01,fr om-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:28 10 .1.0.2 1,2016/11/15 08:47:28 ,001801015967,TRAFFIC,start,
1,2016/11/15 08:47:28,12.167 .43.50,50.232.155.145,12.167 .43.50,10.250.0.10,inbound-
w eb-browsing,,,web-browsing,v sys1,outside,dmz,ethernet1/4 ,ethernet1/2,dell-securework
s,2016/11/15 08:47:28,31435,
1,52746,80,52746,80,0x400000 ,tcp,allow,982,908,74,4,2016 /11/15 08:47:27,1,any,0,2816
310231,0x0,US,US,0,3,1,n/a,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:47:28 10.1.0.2 1,2016/11/15 08:47:28,001801 015967,TRAFFIC,end,1,2016/11 /15
08:47:28,152.133.7.129,5 0.232.155.145,152.133.7.129, 10.250.0.10,inbound-web-brow
sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/ 11/15
08:47:28,15917,1,13962 ,80,13962,80,0x40001a,tcp,al low,17045,5711,11334,23,2016 /11/15
08:47:06,6,government ,0,2816310207,0x0,US,US,0,12 ,11,tcp-rst-from-client,0,0, 0,0,,ATL-
PAN-01,from-policy
Nov 15 08:47:28 10.1.0.2 1,2 016/11/15 08:47:28,001801015 967,TRAFFIC,start,1,2016/11/
15 08:47:28,173.46.76.149,50 .232.155.145,173.46.76.149,1 0.250.0.10,inbound-web-brows
ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1
1/15 08:47:28,32035,1,19867, 80,19867,80,0x400000,tcp,all ow,583,509,74,4,2016/11/15 0
8:47:28,0,any,0,2816310258,0 x0,US,US,0,3,1,n/a,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:47:28 10.1.0.2 1,2016/1 1/15 08:47:28,001801015967,T RAFFIC,end,1,2016/11/15
08:4 7:28,64.85.97.249,50.232.155 .145,64.85.97.249,10.250.0.1 0,inbound-
web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell
-secureworks,2016/11/15 08:4 7:28,32697,1,43234,80,43234,
80,0x40001c,tcp,allow,151779 ,19229,132550,217,2016/11/15 08:47:00,12,government,0,28
16310213,0x0,US,US,0,117,100 ,tcp-rst-from-client,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:47:28 10.1.0.2 1,2016 /11/15 08:47:28,001801015967 ,TRAFFIC,drop,1,2016/11/15
0 8:47:28,175.194.65.27,50.232 .155.145,0.0.0.0,0.0.0.0,den y-remaining,,,not-
applicable ,vsys1,outside,dmz,ethernet1 /4,,dell-secureworks,2016/11 /15
08:47:28,0,1,2951,23,0,0 ,0x0,tcp,deny,60,60,0,1,2016 /11/15 08:47:28,0,any,0,2816
310250,0x0,KR,US,0,1,0,polic y-deny,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:47:28 1 0.1.0.2 1,2016/11/15 08:47:2 8,001801015967,TRAFFIC,start ,1,2016/11/15
08:47:28,173.4 6.76.149,50.232.155.145,173. 46.76.149,10.250.0.10,inboun d-web-
browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew
orks,2016/11/15 08:47:28,526 19,1,19865,80,19865,80,0x400 000,tcp,allow,583,509,74,4,2
016/11/15 08:47:28,0,any,0,2 816310253,0x0,US,US,0,3,1,n/ a,0,0,0,0,,ATL-PAN-01,from-p
olicy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:27 10.1.0 .2 1,2016/11/15 08:47:27,001 801015967,TRAFFIC,start,1,20
16/11/15 08:47:27,209.67.78. 56,50.232.155.145,209.67.78. 56,10.250.0.10,inbound-web-
b rowsing,,,web-browsing,vsys1 ,outside,dmz,ethernet1/4,eth ernet1/2,dell-secureworks,20
16/11/15 08:47:27,44463,1,60 106,80,60106,80,0x400000,tcp ,allow,684,610,74,4,2016/11/ 15
08:47:27,0,any,0,28163101 88,0x0,US,US,0,3,1,n/a,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:47:27 10.1.0.2 1,20 16/11/15 08:47:27,0018010159 67,TRAFFIC,end,1,2016/11/15
08:47:27,74.174.56.6,50.232. 155.145,74.174.56.6,10.250.0 .10,inbound-web-browsing,,,w
eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15
08 :47:27,33017,1,32281,80,3228 1,80,0x40001a,tcp,allow,1428 0,8356,5924,30,2016/11/15
08 :46:24,47,government,0,28163 10118,0x0,US,US,0,18,12,tcp- rst-from-client,0,0,0,0,,ATL -
PAN-01,from-policy
Nov 15 0 8:47:27 10.1.0.2 1,2016/11/1 5 08:47:27,001801015967,TRAF FIC,end,1,2016/11/15
08:47:2 7,74.174.56.6,50.232.155.145 ,74.174.56.6,10.250.0.10,inb ound-web-browsing,,,web-
brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu reworks,2016/11/15 08:47:27,
22988,1,29843,80,29843,80,0x 40001a,tcp,allow,18347,2522, 15825,28,2016/11/15
08:46:23 ,48,government,0,2816310150, 0x0,US,US,0,13,15,tcp-rst-fr om-client,0,0,0,0,,ATL-
PAN-0 1,from-policy
Nov 15 08:47:2 6 10.1.0.2 1,2016/11/15 08:4 7:26,001801015967,TRAFFIC,en d,1,2016/11/15
08:47:26,64.8 5.77.5,50.232.155.145,64.85. 77.5,10.250.0.10,inbound-web -browsing,,,web-
browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15
08:47:26,43358,1, 45574,80,45574,80,0x40001c,t cp,allow,68397,4615,63782,89 ,2016/11/15
08:46:11,59,gove rnment,0,2816310060,0x0,US,U S,0,42,47,tcp-fin,0,0,0,0,,A TL-PAN-01,from-
policy
Nov 15 08:47:27 10.1.0.2 1,2016/11 /15 08:47:27,001801015967,TR AFFIC,end,1,2016/11/15
08:47 :27,74.174.56.6,50.232.155.1 45,74.174.56.6,10.250.0.10,i nbound-web-browsing,,,web-
br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15
08:47:2 7,25943,1,63694,80,63694,80, 0x40001a,tcp,allow,5434,3326 ,2108,15,2016/11/15
08:46:23 ,48,government,0,2816310157, 0x0,US,US,0,10,5,tcp-rst-fro m-client,0,0,0,0,,ATL-
PAN-01 ,from-policy
Nov 15 08:47:26 10.1.0.2 1,2016/11/15 08:47 :26,001801015967,TRAFFIC,end ,1,2016/11/15
08:47:26,68.10 1.63.60,50.232.155.145,68.10 1.63.60,10.250.0.10,inbound-
web-browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-
securewor ks,2016/11/15 08:47:26,35504 ,1,45203,80,45203,80,0x40001
a,tcp,allow,26364,8405,17959 ,34,2016/11/15 08:47:03,7,go

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

vernment,0,2816310064,0x0,US ,US,0,18,16,tcp-rst-from-cli ent,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:47:24 10.1 .0.2 1,2016/11/15 08:47:24,0 01801015967,TRAFFIC,start,1, 2016/11/15 08:47:24,152.133. 7.129,50.232.155.145,152.133 .7.129,10.250.0.10,inbound-w eb-browsing,,,web-browsing,v sys1,outside,dmz,ethernet1/4 ,ethernet1/2,dell-securework s,2016/11/15 08:47:24,48461, 1,11160,80,11160,80,0x400000 ,tcp,allow,1606,1540,66,4,20 16/11/15 08:47:23,0,any,0,28 16309958,0x0,US,US,0,3,1,n/a ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:47:25 10.1.0. 2 1,2016/11/15 08:47:25,0018 01015967,TRAFFIC,end,1,2016/ 11/15 08:47:25,64.85.77.2,50 .232.155.145,64.85.77.2,10.2 50.0.10,inbound-web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5 08:47:25,40469,1,60485,80, 60485,80,0x40001c,tcp,allow, 47545,8386,39159,58,2016/11/ 15 08:46:07,62,government,0, 2816309994,0x0,US,US,0,28,30 ,tcp-fin,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:47:24 10.1.0.2 1,2016/11/15 08:47 :24,001801015967,TRAFFIC,sta rt,1,2016/11/15 08:47:24,152 .133.7.129,50.232.155.145,15 2.133.7.129,10.250.0.10,inbo und-web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:47:24,5 2489,1,33536,80,33536,80,0x4 00000,tcp,allow,1606,1540,66 ,4,2016/11/15 08:47:23,0,any ,0,2816309954,0x0,US,US,0,3, 1,n/a,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:47:24 10 .1.0.2 1,2016/11/15 08:47:24 ,001801015967,TRAFFIC,end,1, 2016/11/15 08:47:24,209.67.7 8.35,50.232.155.145,209.67.7 8.35,10.250.0.10,inbound-web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15 08:47:24,35499,1, 41084,80,41084,80,0x40001c,t cp,allow,70823,9726,61097,90 ,2016/11/15 08:47:07,1,gover nment,0,2816309930,0x0,US,US ,0,44,46,tcp-rst-from-client ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:47:24 10.1.0. 2 1,2016/11/15 08:47:24,0018 01015967,TRAFFIC,end,1,2016/ 11/15 08:47:24,66.192.63.2,5 0.232.155.145,66.192.63.2,10 .250.0.10,inbound-web-browsing,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15 08:47:24,18519,1,41077,8 0,41077,80,0x40001c,tcp,allo w,81427,19438,61989,73,2016/ 11/15 08:44:38,150,governmen t,0,2816309937,0x0,US,US,0,2 8,45,tcp-fin,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 7:23 10.1.0.2 1,2016/11/15 0 8:47:23,001801015967,TRAFFIC ,start,1,2016/11/15 08:47:23 ,152.133.7.129,50.232.155.14 5,152.133.7.129,10.250.0.10, inbound-web-browsing,,,web-b rowsing,vsys1,outside,dmz,et hernet1/4,ethernet1/2,dell-s

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

ecureworks,2016/11/15 08:47: 23,52014,1,61007,80,61007,80 ,0x400000,tcp,allow,1606,154
0,66,4,2016/11/15 08:47:23,0 ,any,0,2816309912,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-0
1,from-policy
Nov 15 08:47:2 3 10.1.0.2 1,2016/11/15 08:4 7:23,001801015967,TRAFFIC,en d,1,2016/11/15
08:47:23,152. 133.7.129,50.232.155.145,152 .133.7.129,10.250.0.10,inbou nd-web-
browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure
works,2016/11/15 08:47:23,16 617,1,61731,80,61731,80,0x40 001a,tcp,allow,4266,2627,163
9,9,2016/11/15 08:47:07,0,go vernment,0,2816309888,0x0,US ,US,0,5,4,tcp-rst-from-clien
t,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:47:23 10.1.0 .2 1,2016/11/15 08:47:23,001 801015967,TRAFFIC,end,1,2016 /11/15
08:47:23,152.133.7.12 9,50.232.155.145,152.133.7.1 29,10.250.0.10,inbound-web-b
rowsing,,,web-browsing,vsys1 ,outside,dmz,ethernet1/4,eth ernet1/2,dell-secureworks,20
16/11/15 08:47:23,45574,1,61 730,80,61730,80,0x40001a,tcp ,allow,4386,2747,1639,11,201
6/11/15 08:47:06,1,governmen t,0,2816309868,0x0,US,US,0,7 ,4,tcp-rst-from-
client,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:47:21 10.1.0.2 1,20 16/11/15 08:47:21,0018010159 67,TRAFFIC,drop,1,2016/11/15
08:47:21,89.248.160.192,50. 232.155.145,0.0.0.0,0.0.0.0, deny-remaining,,,not-applica
ble,vsys1,outside,dmz,ethern et1/4,,dell-secureworks,2016 /11/15 08:47:21,0,1,35047,12
3,0,0,0x0,udp,deny,60,60,0,1 ,2016/11/15 08:47:21,0,any,0 ,2816309770,0x0,SC,US,0,1,0,
policy-deny,0,0,0,0,,ATL-PAN -01,from-policy
Nov 15 08:47 :22 10.1.0.2 1,2016/11/15 08 :47:22,001801015967,TRAFFIC, end,1,2016/11/15
08:47:22,20 9.67.78.50,50.232.155.145,20 9.67.78.50,10.250.0.10,inbou nd-web-
browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure
works,2016/11/15 08:47:22,72 621,1,33411,80,33411,80,0x40 001c,tcp,allow,91602,11886,7
9716,146,2016/11/15 08:46:39 ,27,government,0,2816309824, 0x0,US,US,0,79,67,tcp-rst-fr
om-client,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:47:2 1 10.1.0.2 1,2016/11/15 08:4 7:21,001801015967,TRAFFIC,st art,1,2016/11/15
08:47:21,20 9.67.78.57,50.232.155.145,20 9.67.78.57,10.250.0.10,inbou nd-web-
browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure
works,2016/11/15 08:47:21,30 852,1,51081,80,51081,80,0x40 0000,tcp,allow,650,576,74,4,
2016/11/15 08:47:21,0,any,0, 2816309663,0x0,US,US,0,3,1,n /a,0,0,0,0,,ATL-PAN-01,from-
policy
Nov 15 08:47:21 10.1. 0.2 1,2016/11/15 08:47:21,00 1801015967,TRAFFIC,end,1,201
6/11/15 08:47:21,64.85.77.7, 50.232.155.145,64.85.77.7,10 .250.0.10,inbound-web-browsi

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

ng,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15 08:47:21,15186,1,47653,8 0,47653,80,0x40001c,tcp,allo w,40475,7683,32792,49,2016/1 1/15 08:47:02,3,government,0 ,2816309645,0x0,US,US,0,23,2 6,tcp-rst-from-client,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:47:20 10.1.0.2 1,201 6/11/15 08:47:20,00180101596 7,TRAFFIC,start,1,2016/11/15 08:47:20,66.110.201.211,50. 232.155.145,66.110.201.211,1 0.250.0.10,inbound-web-brows ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15 08:47:20,63592,1,62817, 80,62817,80,0x400000,tcp,all ow,664,590,74,4,2016/11/15 0 8:47:20,0,any,0,2816309622,0 x0,US,US,0,3,1,n/a,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:47:21 10.1.0.2 1,2016/1 1/15 08:47:21,001801015967,T RAFFIC,end,1,2016/11/15 08:4 7:21,152.133.7.129,50.232.15 5.145,152.133.7.129,10.250.0 .10,inbound-web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15 08 :47:21,245542,1,30603,80,306 03,80,0x40001a,tcp,allow,519 91,13831,38160,58,2016/11/15 08:46:57,8,government,0,281 6309651,0x0,US,US,0,25,33,tc p-rst-from-client,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:47:21 10.1.0.2 1,2016/11 /15 08:47:21,001801015967,TR AFFIC,end,1,2016/11/15 08:47 :21,96.86.229.133,50.232.155 .145,96.86.229.133,10.250.0. 10,inbound-web-browsing,,,we b-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08: 47:21,30555,1,63258,80,63258 ,80,0x40001c,tcp,allow,22928 ,5136,17792,42,2016/11/15 08 :46:11,54,government,0,28163 09646,0x0,US,US,0,28,14,tcp- fin,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:47:19 10.1 .0.2 1,2016/11/15 08:47:19,0 01801015967,TRAFFIC,start,1, 2016/11/15 08:47:19,174.218. 143.68,50.232.155.145,174.21 8.143.68,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:47:19,3392 0,1,8159,80,8159,80,0x400000 ,tcp,allow,724,650,74,4,2016 /11/15 08:47:19,0,any,0,2816 309563,0x0,US,US,0,3,1,n/a,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:47:20 10.1.0.2 1,2016/11/15 08:47:20,001801 015967,TRAFFIC,start,1,2016/ 11/15 08:47:20,64.85.97.245, 50.232.155.145,64.85.97.245, 10.250.0.10,inbound-web-brow sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/ 11/15 08:47:20,36013,1,51931 ,80,51931,80,0x400000,tcp,al low,684,610,74,4,2016/11/15 08:47:19,0,any,0,2816309580, 0x0,US,US,0,3,1,n/a,0,0,0,0, ,ATL-PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:19 10.1.0.2 1,2016/ 11/15 08:47:19,001801015967, TRAFFIC,start,1,2016/11/15 0 8:47:19,64.85.77.10,50.232.1 55.145,64.85.77.10,10.250.0. 10,inbound-web-browsing,,,we b-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08: 47:19,34210,1,36583,80,36583 ,80,0x400000,tcp,allow,689,6 15,74,4,2016/11/15 08:47:18, 1,any,0,2816309555,0x0,US,US ,0,3,1,n/a,0,0,0,0,,ATL-PAN- 01,from-policy
Nov 15 08:47: 19 10.1.0.2 1,2016/11/15 08: 47:19,001801015967,TRAFFIC,e nd,1,2016/11/15 08:47:19,47. 32.70.122,50.232.155.145,47. 32.70.122,10.250.0.10,inboun d-web-browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew orks,2016/11/15 08:47:19,955 8,1,54723,80,54723,80,0x4000 1c,tcp,allow,2907,1322,1585, 9,2016/11/15 08:47:02,1,gove rnment,0,2816309550,0x0,US,U S,0,6,3,tcp-rst-from-client, 0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:47:19 10.1.0.2 1,2016/11/15 08:47:19,00180 1015967,TRAFFIC,end,1,2016/1 1/15 08:47:19,209.67.78.49,5 0.232.155.145,209.67.78.49,1 0.250.0.10,inbound-web-brows ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15 08:47:19,34654,1,49351, 80,49351,80,0x40001c,tcp,all ow,5080,1723,3357,15,2016/11 /15 08:47:00,3,government,0, 2816309544,0x0,US,US,0,10,5, tcp-rst-from-client,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:47:17 10.1.0.2 1,2016/ 11/15 08:47:17,001801015967, TRAFFIC,end,1,2016/11/15 08: 47:17,64.179.192.42,50.232.1 55.145,64.179.192.42,10.250. 0.10,inbound-web-browsing,,, web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0 8:47:17,43720,1,40016,80,400 16,80,0x40001a,tcp,allow,205 192,30197,174995,267,2016/11 /15 08:46:22,39,government,0 ,2816309377,0x0,US,US,0,139, 128,tcp-rst-from-client,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:47:17 10.1.0.2 1,2 016/11/15 08:47:17,001801015 967,TRAFFIC,end,1,2016/11/15 08:47:17,74.183.101.197,50. 232.155.145,74.183.101.197,1 0.250.0.10,inbound-web-brows ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15 08:47:17,47062,1,53629, 80,53629,80,0x40001c,tcp,all ow,5055,979,4076,14,2016/11/ 15 08:46:50,11,government,0, 2816309378,0x0,US,US,0,8,6,t cp-fin,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:47:17 1 0.1.0.2 1,2016/11/15 08:47:1 7,001801015967,TRAFFIC,start ,1,2016/11/15 08:47:17,66.19 2.63.2,50.232.155.145,66.192 .63.2,10.250.0.10,inbound-we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-secureworks ,2016/11/15 08:47:17,26984,1 ,29063,80,29063,80,0x400000, tcp,allow,1523,1449,74,4,201 6/11/15 08:47:17,0,any,0,281 6309421,0x0,US,US,0,3,1,n/a, 0,0,0,0,,ATL-PAN-01,from-pol icy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:17 10.1.0.2 1,2016/11/15 08:47:17,00180 1015967,TRAFFIC,end,1,2016/1 1/15 08:47:17,64.85.77.9,50. 232.155.145,64.85.77.9,10.25 0.0.10,inbound-web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15 08:47:17,26998,1,47431,80,4 7431,80,0x40001c,tcp,allow,4 0678,2714,37964,54,2016/11/1 5 08:46:59,2,government,0,28 16309376,0x0,US,US,0,26,28,t cp-rst-from-client,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:47:16 10.1.0.2 1,2016/1 1/15 08:47:16,001801015967,T RAFFIC,end,1,2016/11/15 08:4 7:16,64.85.97.176,50.232.155 .145,64.85.97.176,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4 7:16,46645,1,52855,80,52855, 80,0x40001c,tcp,allow,13776, 4076,9700,30,2016/11/15 08:4 6:38,22,government,0,2816309 277,0x0,US,US,0,20,10,tcp-fi n,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:47:16 10.1.0 .2 1,2016/11/15 08:47:16,001 801015967,TRAFFIC,end,1,2016 /11/15 08:47:16,172.56.5.57, 50.232.155.145,172.56.5.57,1 0.250.0.10,inbound-web-brows ing,,,incomplete,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15 08:47:16,41862,1,62300,80 ,62300,80,0x40001b,tcp,allow ,340,206,134,5,2016/11/15 08 :46:50,10,any,0,2816309269,0 x0,US,US,0,3,2,tcp-rst-from- server,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:47:15 1 0.1.0.2 1,2016/11/15 08:47:1 5,001801015967,TRAFFIC,start ,1,2016/11/15 08:47:15,209.6 7.78.48,50.232.155.145,209.6 7.78.48,10.250.0.10,inbound- web-browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-secureworks,2016/11/15 08:47:15,30287 ,1,38032,80,38032,80,0x40000 0,tcp,allow,684,610,74,4,201 6/11/15 08:47:15,0,any,0,281 6309220,0x0,US,US,0,3,1,n/a, 0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:47:15 10.1.0.2 1,2016/11/15 08:47:15,00180 1015967,TRAFFIC,end,1,2016/1 1/15 08:47:15,205.173.105.20 5,50.232.155.145,205.173.105 .205,10.250.0.10,inbound-web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15 08:47:15,29465,1, 54562,80,54562,80,0x40001a,t cp,allow,2104,525,1579,8,201 6/11/15 08:46:31,28,governme nt,0,2816309171,0x0,US,US,0, 5,3,tcp-rst-from-client,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:47:14 10.1.0.2 1,2 016/11/15 08:47:14,001801015 967,TRAFFIC,end,1,2016/11/15 08:47:14,108.66.253.68,50.2 32.155.145,108.66.253.68,10. 250.0.10,inbound-web-browsing,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15 08:47:14,42763,1,60738,80 ,60738,80,0x40001c,tcp,allow ,173062,14728,158334,184,201

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

6/11/15 08:45:35,83,governme nt,0,2816309061,0x0,US,US,0, 66,118,tcp-rst-from-client,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:47:14 10.1.0.2 1,2016/11/15 08:47:14,001801 015967,TRAFFIC,end,1,2016/11 /15 08:47:14,64.179.192.42,5 0.232.155.145,64.179.192.42, 10.250.0.10,inbound-web-brow sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/ 11/15 08:47:14,35247,1,34493 ,80,34493,80,0x40001a,tcp,al low,2704,1179,1525,7,2016/11 /15 08:46:58,0,government,0, 2816309046,0x0,US,US,0,5,2,t cp-rst-from-client,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:47:14 10.1.0.2 1,2016/1 1/15 08:47:14,001801015967,T RAFFIC,start,1,2016/11/15 08 :47:14,152.133.7.129,50.232. 155.145,152.133.7.129,10.250 .0.10,inbound-web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15 08:47:14,12205,1,54312,80,54 312,80,0x400000,tcp,allow,16 06,1540,66,4,2016/11/15 08:4 7:13,0,any,0,2816309038,0x0, US,US,0,3,1,n/a,0,0,0,0,,ATL - PAN-01,from-policy
Nov 15 0 8:47:13 10.1.0.2 1,2016/11/1 5 08:47:13,001801015967,TRAF FIC,end,1,2016/11/15 08:47:1 3,152.133.7.129,50.232.155.1 45,152.133.7.129,10.250.0.10 ,inbound-web-browsing,,,web- browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell-secureworks,2016/11/15 08:47 :13,18634,1,45077,80,45077,8 0,0x40001a,tcp,allow,87891,9 412,78479,103,2016/11/15 08: 46:22,35,government,0,281630 8988,0x0,US,US,0,41,62,tcp-r st-from-client,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :47:13 10.1.0.2 1,2016/11/15 08:47:13,001801015967,TRAFF IC,start,1,2016/11/15 08:47: 13,152.133.7.129,50.232.155. 145,152.133.7.129,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell - secureworks,2016/11/15 08:4 7:13,41230,1,24538,80,24538, 80,0x400000,tcp,allow,1606,1 540,66,4,2016/11/15 08:47:13 ,0,any,0,2816309029,0x0,US,U S,0,3,1,n/a,0,0,0,0,,ATL-PAN -01,from-policy
Nov 15 08:47 :12 10.1.0.2 1,2016/11/15 08 :47:12,001801015967,TRAFFIC, end,1,2016/11/15 08:47:12,15 2.133.7.129,50.232.155.145,1 52.133.7.129,10.250.0.10,inb ound-web-browsing,,,web-brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu reworks,2016/11/15 08:47:12, 45581,1,61700,80,61700,80,0x 40001a,tcp,allow,17038,5711, 11327,23,2016/11/15 08:45:51 ,65,government,0,2816308912, 0x0,US,US,0,12,11,tcp-rst-fr om-client,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:47:1 2 10.1.0.2 1,2016/11/15 08:4 7:12,001801015967,TRAFFIC,en d,1,2016/11/15 08:47:12,162. 17.64.145,50.232.155.145,162 .17.64.145,10.250.0.10,inbou nd-web-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure works,2016/11/15 08:47:12,37 046,1,49744,80,49744,80,0x40 001a,tcp,allow,94422,8999,85 423,106,2016/11/15 08:46:32, 24,government,0,2816308895,0 x0,US,US,0,31,75,tcp-rst-fro m-client,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:47:12 10.1.0.2 1,2016/11/15 08:47 :12,001801015967,TRAFFIC,end ,1,2016/11/15 08:47:12,107.7 7.90.82,50.232.155.145,107.7 7.90.82,10.250.0.10,inbound-web-browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-securewor ks,2016/11/15 08:47:12,41183 ,1,42958,80,42958,80,0x40001 c,tcp,allow,15438,3530,11908 ,30,2016/11/15 08:46:54,2,go vernment,0,2816308926,0x0,US ,US,0,20,10,tcp-fin,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:47:12 10.1.0.2 1,2016/ 11/15 08:47:12,001801015967, TRAFFIC,start,1,2016/11/15 0 8:47:12,64.179.192.42,50.232 .155.145,64.179.192.42,10.25 0.0.10,inbound-web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15 08:47:12,36698,1,57922,80,5 7922,80,0x400000,tcp,allow,1 203,1137,66,4,2016/11/15 08: 47:01,11,any,0,2816308942,0x 0,US,US,0,3,1,n/a,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:47:11 10.1.0.2 1,2016/11 /15 08:47:11,001801015967,TR AFFIC,start,1,2016/11/15 08: 47:11,74.174.56.6,50.232.155 .145,74.174.56.6,10.250.0.10 ,inbound-web-browsing,,,web-browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell- secureworks,2016/11/15 08:47 :11,51636,1,63746,80,63746,8 0,0x400000,tcp,allow,1165,10 99,66,4,2016/11/15 08:47:11, 0,any,0,2816308859,0x0,US,US ,0,3,1,n/a,0,0,0,0,,ATL-PAN- 01,from-policy
Nov 15 08:47: 12 10.1.0.2 1,2016/11/15 08: 47:12,001801015967,TRAFFIC,e nd,1,2016/11/15 08:47:12,171 .159.64.10,50.232.155.145,17 1.159.64.10,10.250.0.10,inbo und-web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:47:12,2 2718,1,10001,80,10001,80,0x4 0001c,tcp,allow,5810,1759,40 51,15,2016/11/15 08:46:55,1, government,0,2816308899,0x0, US,US,0,9,6,tcp-fin,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:47:11 10.1.0.2 1,2016/ 11/15 08:47:11,001801015967, TRAFFIC,end,1,2016/11/15 08: 47:11,107.77.90.82,50.232.15 5.145,107.77.90.82,10.250.0. 10,inbound-web-browsing,,,web-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08: 47:11,20097,1,19717,80,19717 ,80,0x40001c,tcp,allow,30778 ,1247,29531,34,2016/11/15 08 :46:54,1,government,0,281630 8784,0x0,US,US,0,12,22,tcp-f in,0,0,0,0,,ATL-PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:11 10.1. 0.2 1,2016/11/15 08:47:11,00 1801015967,TRAFFIC,end,1,201
6/11/15 08:47:11,171.159.64. 10,50.232.155.145,171.159.64 .10,10.250.0.10,inbound-web-
browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2
016/11/15 08:47:11,54861,1,1 0000,80,10000,80,0x40001c,tc p,allow,32820,1818,31002,39,
2016/11/15 08:46:55,0,govern ment,0,2816308765,0x0,US,US, 0,16,23,tcp-fin,0,0,0,0,,ATL -
PAN-01,from-policy
Nov 15 0 8:47:11 10.1.0.2 1,2016/11/1 5 08:47:11,001801015967,TRAF FIC,end,1,2016/11/15
08:47:1 1,209.67.78.50,50.232.155.14 5,209.67.78.50,10.250.0.10,i nbound-web-
browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se
cureworks,2016/11/15 08:47:1 1,37742,1,36960,80,36960,80, 0x40001c,tcp,allow,2323,712,
1611,9,2016/11/15 08:46:55,0 ,government,0,2816308821,0x0 ,US,US,0,6,3,tcp-rst-from-cl
ient,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:47:11 10. 1.0.2 1,2016/11/15 08:47:11, 001801015967,TRAFFIC,start,1 ,2016/11/15
08:47:11,64.85.7 7.5,50.232.155.145,64.85.77. 5,10.250.0.10,inbound-web-br owsing,,,web-
browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201 6/11/15
08:47:11,51740,1,381 14,80,38114,80,0x400000,tcp, allow,684,610,74,4,2016/11/1 5
08:47:10,0,any,0,281630884 4,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:47:10 10.1.0.2 1,201 6/11/15 08:47:10,00180101596 7,TRAFFIC,end,1,2016/11/15
0 8:47:10,173.14.221.37,50.232 .155.145,173.14.221.37,10.25 0.0.10,inbound-
web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-
secureworks,2016/11/15 08:47:10,22665,1,62532,80,6 2532,80,0x40001b,tcp,allow,3
0609,3052,27557,44,2016/11/1 5 08:44:19,155,government,0,
2816308693,0x0,US,US,0,18,26 ,tcp-rst-from-server,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:47:10 10.1.0.2 1,2016 /11/15 08:47:10,001801015967 ,TRAFFIC,end,1,2016/11/15
08 :47:10,158.111.236.10,50.232 .155.145,158.111.236.10,10.2 50.0.10,inbound-
web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-
secureworks,2016/11/1 5 08:47:10,45758,1,28219,80, 28219,80,0x40001a,tcp,allow,
43468,2154,41314,47,2016/11/ 15 08:46:38,16,government,0,
2816308702,0x0,US,US,0,17,30 ,tcp-rst-from-client,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:47:10 10.1.0.2 1,2016 /11/15 08:47:10,001801015967 ,TRAFFIC,end,1,2016/11/15
08 :47:10,158.111.236.10,50.232 .155.145,158.111.236.10,10.2 50.0.10,inbound-
web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-
secureworks,2016/11/1 5 08:47:10,43178,1,38695,80, 38695,80,0x40001a,tcp,allow,

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

93144,9899,83245,88,2016/11/ 15 08:46:38,16,government,0,
2816308692,0x0,US,US,0,28,60 ,tcp-rst-from-client,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:47:10 10.1.0.2 1,2016 /11/15 08:47:10,001801015967 ,TRAFFIC,start,1,2016/11/15
08:47:10,64.85.77.6,50.232.1 55.145,64.85.77.6,10.250.0.1 0,inbound-web-browsing,,,web
-browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15
08:4 7:10,27007,1,33919,80,33919, 80,0x400000,tcp,allow,603,52 9,74,4,2016/11/15
08:47:10,0 ,any,0,2816308740,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:47:0 9 10.1.0.2 1,2016/11/15 08:4 7:09,001801015967,TRAFFIC,en d,1,2016/11/15
08:47:09,209. 67.78.36,50.232.155.145,209. 67.78.36,10.250.0.10,inbound -web-
browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo
rks,2016/11/15 08:47:09,1572 0,1,50013,80,50013,80,0x4000 1c,tcp,allow,47136,5795,4134
1,78,2016/11/15 08:46:40,13, government,0,2816308632,0x0, US,US,0,44,34,tcp-rst-from-c
lient,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:47:09 10 .1.0.2 1,2016/11/15 08:47:09 ,001801015967,TRAFFIC,start,
1,2016/11/15 08:47:09,209.67 .78.56,50.232.155.145,209.67 .78.56,10.250.0.10,inbound-
w eb-browsing,,,web-browsing,v sys1,outside,dmz,ethernet1/4 ,ethernet1/2,dell-securework
s,2016/11/15 08:47:09,153367 ,1,57386,80,57386,80,0x40000 0,tcp,allow,703,629,74,4,201
6/11/15 08:47:08,0,any,0,281 6308626,0x0,US,US,0,3,1,n/a, 0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:47:09 10.1.0.2 1,2016/11/15 08:47:09,00180 1015967,TRAFFIC,start,1,2016 /11/15
08:47:09,209.67.78.55 ,50.232.155.145,209.67.78.55 ,10.250.0.10,inbound-
web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-
secureworks,2016 /11/15 08:47:09,37585,1,5815 2,80,58152,80,0x400000,tcp,a
llow,693,619,74,4,2016/11/15 08:47:08,0,any,0,2816308641 ,0x0,US,US,0,3,1,n/
a,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:47:07 10.1.0.2 1,2016 /11/15 08:47:07,001801015967 ,TRAFFIC,start,1,2016/11/15
08:47:07,209.67.78.35,50.232 .155.145,209.67.78.35,10.250 .0.10,inbound-
web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-
secureworks,2016/11/15 08:47:07,35499,1,41084,80,41 084,80,0x400000,tcp,allow,68
4,610,74,4,2016/11/15 08:47: 07,0,any,0,2816308558,0x0,US ,US,0,3,1,n/a,0,0,0,0,,ATL-P
AN-01,from-policy
Nov 15 08: 47:08 10.1.0.2 1,2016/11/15 08:47:08,001801015967,TRAFFI C,end,1,2016/11/15
08:47:08, 162.17.64.145,50.232.155.145 ,162.17.64.145,10.250.0.10,i nbound-
web-browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-
se cureworks,2016/11/15 08:47:0 8,16856,1,49745,80,49745,80,

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

0x40001a,tcp,allow,5728,1851 ,3877,25,2016/11/15 08:46:32 ,20,government,0,2816308578,
0x0,US,US,0,11,14,tcp-rst-fr om-client,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:47:0 7 10.1.0.2 1,2016/11/15 08:4 7:07,001801015967,TRAFFIC,st art,1,2016/11/15
08:47:07,15 2.133.7.129,50.232.155.145,1 52.133.7.129,10.250.0.10,inb ound-
web-browsing,,,web-brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu
reworks,2016/11/15 08:47:07, 16617,1,61731,80,61731,80,0x 400000,tcp,allow,1606,1540,6
6,4,2016/11/15 08:47:07,0,an y,0,2816308556,0x0,US,US,0,3 ,1,n/a,0,0,0,0,,ATL-PAN-01,f
rom-policy
Nov 15 08:47:07 1 0.1.0.2 1,2016/11/15 08:47:0 7,001801015967,TRAFFIC,start ,1,2016/11/15
08:47:07,152.1 33.7.129,50.232.155.145,152. 133.7.129,10.250.0.10,inboun d-
web-browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-
securew orks,2016/11/15 08:47:07,455 74,1,61730,80,61730,80,0x400
000,tcp,allow,1606,1540,66,4 ,2016/11/15 08:47:06,1,any,0 ,2816308553,0x0,US,US,0,3,1, n/
a,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:47:07 10.1 .0.2 1,2016/11/15 08:47:07,0 01801015967,TRAFFIC,end,1,20
16/11/15 08:47:07,64.85.77.6 ,50.232.155.145,64.85.77.6,1 0.250.0.10,inbound-web-brows
ing,,,incomplete,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/
15 08:47:07,40322,1,50697,80 ,50697,80,0x40001b,tcp,allow ,340,206,134,5,2016/11/15
08 :46:51,0,any,0,2816308512,0x 0,US,US,0,3,2,tcp-rst-from-s erver,0,0,0,0,,ATL-PAN-01,fr
om-policy
Nov 15 08:47:07 10 .1.0.2 1,2016/11/15 08:47:07 ,001801015967,TRAFFIC,start, 1,2016/11/15
08:47:07,152.13 3.7.129,50.232.155.145,152.1 33.7.129,10.250.0.10,inbound -web-
browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo
rks,2016/11/15 08:47:07,1591 7,1,13962,80,13962,80,0x4000 00,tcp,allow,1606,1540,66,4,
2016/11/15 08:47:06,1,any,0, 2816308535,0x0,US,US,0,3,1,n /a,0,0,0,0,,ATL-PAN-01,from-
policy
Nov 15 08:47:06 10.1. 0.2 1,2016/11/15 08:47:06,00 1801015967,TRAFFIC,end,1,201
6/11/15 08:47:06,64.85.77.4, 50.232.155.145,64.85.77.4,10 .250.0.10,inbound-web-browsi
ng,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15
08:47:06,41812,1,32781,8 0,32781,80,0x40001c,tcp,allo w,67327,5058,62269,90,2016/1 1/15
08:46:20,30,government, 0,2816308465,0x0,US,US,0,44, 46,tcp-rst-from-client,0,0,0 ,0,,ATL-
PAN-01,from-policy
N ov 15 08:47:06 10.1.0.2 1,20 16/11/15 08:47:06,0018010159 67,TRAFFIC,end,1,2016/11/15
08:47:06,64.85.97.253,50.232 .155.145,64.85.97.253,10.250 .0.10,inbound-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15 08:47:06,32082,1,45056,80,45 056,80,0x40001c,tcp,allow,28 95,1809,1086,15,2016/11/15 0 8:46:48,2,government,0,28163 08464,0x0,US,US,0,10,5,tcp-f in,0,0,0,0,,ATL-PAN-01,from- policy
Nov 15 08:47:06 10.1. 0.2 1,2016/11/15 08:47:06,00 1801015967,TRAFFIC,start,1,2 016/11/15 08:47:06,12.206.16 .210,50.232.155.145,12.206.1 6.210,10.250.0.10,inbound-we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-secureworks ,2016/11/15 08:47:06,33048,1 ,52453,80,52453,80,0x400000, tcp,allow,593,527,66,4,2016/ 11/15 08:47:06,0,any,0,28163 08487,0x0,US,US,0,3,1,n/a,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:47:05 10.1.0.2 1 ,2016/11/15 08:47:05,0018010 15967,TRAFFIC,end,1,2016/11/ 15 08:47:05,108.230.50.182,5 0.232.155.145,108.230.50.182 ,10.250.0.10,inbound-web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:47:05,36922,1,5959 5,80,59595,80,0x40001b,tcp,a llow,40036,3815,36221,55,201 6/11/15 08:43:49,180,governm ent,0,2816308441,0x0,US,US,0 ,23,32,tcp-rst-from-server,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:47:05 10.1.0.2 1,2016/11/15 08:47:05,001801 015967,TRAFFIC,end,1,2016/11 /15 08:47:05,64.85.77.10,50. 232.155.145,64.85.77.10,10.2 50.0.10,inbound-web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5 08:47:05,39032,1,41856,80, 41856,80,0x40001c,tcp,allow, 4910,2287,2623,18,2016/11/15 08:46:20,29,government,0,28 16308422,0x0,US,US,0,12,6,tc p-fin,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:47:05 10 .1.0.2 1,2016/11/15 08:47:05 ,001801015967,TRAFFIC,start, 1,2016/11/15 08:47:05,152.13 3.7.129,50.232.155.145,152.1 33.7.129,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:47:05,2455 42,1,30603,80,30603,80,0x400 000,tcp,allow,1606,1540,66,4 ,2016/11/15 08:46:57,7,any,0 ,2816308414,0x0,US,US,0,3,1, n/ a,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:47:03 10.1 .0.2 1,2016/11/15 08:47:03,0 01801015967,TRAFFIC,start,1, 2016/11/15 08:47:03,68.101.6 3.60,50.232.155.145,68.101.6 3.60,10.250.0.10,inbound-web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15 08:47:03,32454,1, 37191,80,37191,80,0x400000,t cp,allow,566,500,66,4,2016/1 1/15 08:47:02,0,any,0,281630 8306,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:03 10.1.0.2 1, 2016/11/15 08:47:03,00180101 5967,TRAFFIC,start,1,2016/11 /15 08:47:03,66.192.63.2,50. 232.155.145,66.192.63.2,10.2 50.0.10,inbound-web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5 08:47:03,60339,1,11402,80, 11402,80,0x400000,tcp,allow, 1523,1449,74,4,2016/11/15 08 :47:02,1,any,0,2816308320,0x 0,US,US,0,3,1,n/a,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:47:03 10.1.0.2 1,2016/11 /15 08:47:03,001801015967,TR AFFIC,start,1,2016/11/15 08: 47:03,68.101.63.60,50.232.15 5.145,68.101.63.60,10.250.0. 10,inbound-web-browsing,,,web-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08: 47:03,35504,1,45203,80,45203 ,80,0x400000,tcp,allow,678,6 12,66,4,2016/11/15 08:47:03, 0,any,0,2816308322,0x0,US,US ,0,3,1,n/a,0,0,0,0,,ATL-PAN- 01,from-policy
Nov 15 08:47: 03 10.1.0.2 1,2016/11/15 08: 47:03,001801015967,TRAFFIC,s tart,1,2016/11/15 08:47:03,6 4.85.77.7,50.232.155.145,64. 85.77.7,10.250.0.10,inbound- web-browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-securewor ks,2016/11/15 08:47:03,15186 ,1,47653,80,47653,80,0x40000 0,tcp,allow,684,610,74,4,201 6/11/15 08:47:02,0,any,0,281 6308271,0x0,US,US,0,3,1,n/a, 0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:47:03 10.1.0.2 1,2016/11/15 08:47:03,00180 1015967,TRAFFIC,start,1,2016 /11/15 08:47:03,47.32.70.122 ,50.232.155.145,47.32.70.122 ,10.250.0.10,inbound-web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:47:03,9558,1,54723 ,80,54723,80,0x400000,tcp,al low,1208,1142,66,4,2016/11/1 5 08:47:02,0,any,0,281630831 4,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:47:02 10.1.0.2 1,201 6/11/15 08:47:02,00180101596 7,TRAFFIC,end,1,2016/11/15 0 8:47:02,66.192.63.2,50.232.1 55.145,66.192.63.2,10.250.0. 10,inbound-web-browsing,,,web-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08: 47:02,42068,1,23777,80,23777 ,80,0x40001c,tcp,allow,81009 ,17549,63460,77,2016/11/15 0 8:45:39,67,government,0,2816 308226,0x0,US,US,0,31,46,tcp -fin,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:47:02 10. 1.0.2 1,2016/11/15 08:47:02, 001801015967,TRAFFIC,start,1 ,2016/11/15 08:47:02,47.32.7 0.122,50.232.155.145,47.32.7 0.122,10.250.0.10,inbound-we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-secureworks ,2016/11/15 08:47:02,32993,1 ,54724,80,54724,80,0x400000, tcp,allow,1218,1152,66,4,201 6/11/15 08:47:02,0,any,0,281 6308257,0x0,US,US,0,3,1,n/a, 0,0,0,0,,ATL-PAN-01,from-pol icy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:01 10.1.0.2 1,2016/11/15 08:47:01,00180 1015967,TRAFFIC,end,1,2016/1 1/15 08:47:01,64.85.77.2,50. 232.155.145,64.85.77.2,10.25 0.0.10,inbound-web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15 08:47:01,29536,1,60310,80,6 0310,80,0x40001c,tcp,allow,3 6691,6907,29784,39,2016/11/1 5 08:45:45,60,government,0,2 816308163,0x0,US,US,0,16,23, tcp-fin,0,0,0,0,,ATL-PAN-01, from-policy
Nov 15 08:47:01 10.1.0.2 1,2016/11/15 08:47: 01,001801015967,TRAFFIC,star t,1,2016/11/15 08:47:01,64.8 5.97.249,50.232.155.145,64.8 5.97.249,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:47:01,3269 7,1,43234,80,43234,80,0x4000 00,tcp,allow,684,610,74,4,20 16/11/15 08:47:00,0,any,0,28 16308135,0x0,US,US,0,3,1,n/a ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:47:00 10.1.0. 2 1,2016/11/15 08:47:00,0018 01015967,TRAFFIC,end,1,2016/ 11/15 08:47:00,162.95.216.22 2,50.232.155.145,162.95.216. 222,10.250.0.10,inbound-web-browsing,,,incomplete,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201 6/11/15 08:47:00,13527,1,162 19,80,16219,80,0x40001b,tcp, allow,264,138,126,4,2016/11/ 15 08:44:33,131,any,0,281630 8086,0x0,US,US,0,2,2,tcp-rst -from-server,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 7:00 10.1.0.2 1,2016/11/15 0 8:47:00,001801015967,TRAFFIC ,end,1,2016/11/15 08:47:00,1 62.95.216.222,50.232.155.145 ,162.95.216.222,10.250.0.10, inbound-web-browsing,,,web-b rowsing,vsys1,outside,dmz,et hernet1/4,ethernet1/2,dell-s ecureworks,2016/11/15 08:47: 00,33507,1,16211,80,16211,80 ,0x40001b,tcp,allow,30342,10 65,29277,35,2016/11/15 08:44 :33,131,government,0,2816308 065,0x0,US,US,0,13,22,tcp-rs t-from-server,0,0,0,0,,ATL-P AN-01,from-policy
Nov 15 08: 47:00 10.1.0.2 1,2016/11/15 08:47:00,001801015967,TRAFFI C,start,1,2016/11/15 08:47:0 0,64.85.77.9,50.232.155.145, 64.85.77.9,10.250.0.10,inbou nd-web-browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure works,2016/11/15 08:47:00,26 998,1,47431,80,47431,80,0x40 0000,tcp,allow,612,538,74,4, 2016/11/15 08:46:59,0,any,0, 2816308039,0x0,US,US,0,3,1,n /a,0,0,0,0,,ATL-PAN-01,from- policy
Nov 15 08:47:00 10.1. 0.2 1,2016/11/15 08:47:00,00 1801015967,TRAFFIC,start,1,2 016/11/15 08:47:00,209.67.78 .49,50.232.155.145,209.67.78 .49,10.250.0.10,inbound-web-browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2 016/11/15 08:47:00,34654,1,4 9351,80,49351,80,0x400000,tc p,allow,618,544,74,4,2016/11 /15 08:47:00,0,any,0,2816308 117,0x0,US,US,0,3,1,n/a,0,0, 0,0,,ATL-PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:47:00 10.1.0.2 1,2 016/11/15 08:47:00,001801015 967,TRAFFIC,end,1,2016/11/15 08:47:00,162.95.216.222,50. 232.155.145,162.95.216.222,1 0.250.0.10,inbound-web-brows ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15 08:47:00,34247,1,16212, 80,16212,80,0x40001b,tcp,all ow,17692,1328,16364,23,2016/ 11/15 08:44:33,131,governmen t,0,2816308085,0x0,US,US,0,9 ,14,tcp-rst-from-server,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:59 10.1.0.2 1,2 016/11/15 08:46:59,001801015 967,TRAFFIC,start,1,2016/11/ 15 08:46:59,64.179.192.42,50 .232.155.145,64.179.192.42,1 0.250.0.10,inbound-web-brows ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15 08:46:59,35247,1,34493, 80,34493,80,0x400000,tcp,all ow,1125,1059,66,4,2016/11/15 08:46:58,0,any,0,2816307997 ,0x0,US,US,0,3,1,n/a,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:46:59 10.1.0.2 1,2016 /11/15 08:46:59,001801015967 ,TRAFFIC,start,1,2016/11/15 08:46:59,205.173.105.205,50. 232.155.145,205.173.105.205, 10.250.0.10,inbound-web-brow sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/ 11/15 08:46:59,29465,1,54562 ,80,54562,80,0x400000,tcp,al low,471,405,66,4,2016/11/15 08:46:31,28,any,0,2816308033 ,0x0,US,US,0,3,1,n/a,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:46:59 10.1.0.2 1,2016 /11/15 08:46:59,001801015967 ,TRAFFIC,start,1,2016/11/15 08:46:59,64.85.77.4,50.232.1 55.145,64.85.77.4,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4 6:59,52280,1,43809,80,43809, 80,0x400000,tcp,allow,693,61 9,74,4,2016/11/15 08:46:58,0 ,any,0,2816307998,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:46:5 9 10.1.0.2 1,2016/11/15 08:4 6:59,001801015967,TRAFFIC,st art,1,2016/11/15 08:46:59,20 5.173.105.205,50.232.155.145 ,205.173.105.205,10.250.0.10 ,inbound-web-browsing,,,web- browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell-secureworks,2016/11/15 08:46 :59,21025,1,58177,80,58177,8 0,0x400000,tcp,allow,756,690 ,66,4,2016/11/15 08:46:31,28 ,any,0,2816308028,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:46:5 8 10.1.0.2 1,2016/11/15 08:4 6:58,001801015967,TRAFFIC,st art,1,2016/11/15 08:46:58,10 8.66.253.68,50.232.155.145,1 08.66.253.68,10.250.0.10,inb ound-web-browsing,,,web-brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu reworks,2016/11/15 08:46:58, 47496,1,60777,80,60777,80,0x 400000,tcp,allow,790,724,66, 4,2016/11/15 08:46:58,0,any, 0,2816307984,0x0,US,US,0,3,1 ,n/a,0,0,0,0,,ATL-PAN-01,fro m-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:46:57 10. 1.0.2 1,2016/11/15 08:46:57, 001801015967,TRAFFIC,end,1,2
016/11/15 08:46:57,47.32.70. 122,50.232.155.145,47.32.70. 122,10.250.0.10,inbound-web-
browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2
016/11/15 08:46:57,39270,1,5 4722,80,54722,80,0x40001a,tc p,allow,2700,1175,1525,6,201
6/11/15 08:46:40,1,governmen t,0,2816307892,0x0,US,US,0,4 ,2,tcp-rst-from-
client,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:46:55 10.1.0.2 1,20 16/11/15 08:46:55,0018010159 67,TRAFFIC,start,1,2016/11/1
5 08:46:55,171.159.64.10,50. 232.155.145,171.159.64.10,10 .250.0.10,inbound-web-browsi
ng,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15
08:46:55,261048,1,10002, 80,10002,80,0x400000,tcp,all ow,728,654,74,4,2016/11/15 0
8:46:55,0,any,0,2816307765,0 x0,US,US,0,3,1,n/a,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:46:56 10.1.0.2 1,2016/1 1/15 08:46:56,001801015967,T RAFFIC,start,1,2016/11/15
08 :46:56,209.67.78.50,50.232.1 55.145,209.67.78.50,10.250.0 .10,inbound-web-browsing,,,w
eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15
08 :46:56,37742,1,36960,80,3696 0,80,0x400000,tcp,allow,600, 526,74,4,2016/11/15
08:46:55 ,0,any,0,2816307778,0x0,US,U S,0,3,1,n/a,0,0,0,0,,ATL-PAN -01,from-policy
Nov 15 08:46 :56 10.1.0.2 1,2016/11/15 08 :46:56,001801015967,TRAFFIC, end,1,2016/11/15
08:46:56,17 4.218.133.21,50.232.155.145, 174.218.133.21,10.250.0.10,i nbound-
web-browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se
cureworks,2016/11/15 08:46:5 6,49120,1,2529,80,2529,80,0x 40001c,tcp,allow,31719,2122,
29597,49,2016/11/15 08:46:36 ,4,government,0,2816307790,0 x0,US,US,0,26,23,tcp-
fin,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:55 10.1.0.2 1, 2016/11/15 08:46:55,00180101 5967,TRAFFIC,start,1,2016/11 /15
08:46:55,171.159.64.10,5 0.232.155.145,171.159.64.10, 10.250.0.10,inbound-web-brow
sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/
11/15 08:46:55,22718,1,10001 ,80,10001,80,0x400000,tcp,al low,702,628,74,4,2016/11/15
08:46:55,0,any,0,2816307761, 0x0,US,US,0,3,1,n/a,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:46:56 10.1.0.2 1,2016/ 11/15 08:46:56,001801015967, TRAFFIC,end,1,2016/11/15
08: 46:56,104.182.206.4,50.232.1 55.145,104.182.206.4,10.250. 0.10,inbound-web-browsing,,,
web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0
8:46:56,43140,1,63265,80,632 65,80,0x40001a,tcp,allow,779 63,19171,58792,90,2016/11/15
08:46:24,16,government,0,28 16307796,0x0,US,US,0,44,46,t cp-rst-from-client,0,0,0,0,, ATL-
PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 1 5 08:46:56 10.1.0.2 1,2016/1 1/15 08:46:56,001801015967,T RAFFIC,end,1,2016/11/15 08:4 6:56,47.32.70.122,50.232.155 .145,47.32.70.122,10.250.0.1 0,inbound-web-browsing,,,inc omplete,vsys1,outside,dmz,et hernet1/4,ethernet1/2,dell-s ecureworks,2016/11/15 08:46: 56,44850,1,54719,80,54719,80 ,0x40001b,tcp,allow,312,186, 126,5,2016/11/15 08:46:29,11 ,any,0,2816307794,0x0,US,US, 0,3,2,tcp-rst-from-server,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:46:55 10.1.0.2 1 ,2016/11/15 08:46:55,0018010 15967,TRAFFIC,end,1,2016/11/ 15 08:46:55,174.218.133.21,5 0.232.155.145,174.218.133.21 ,10.250.0.10,inbound-web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:46:55,48359,1,1049 1,80,10491,80,0x40001c,tcp,a llow,19562,4052,15510,49,201 6/11/15 08:46:37,2,governmen t,0,2816307703,0x0,US,US,0,2 7,22,tcp-fin,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 6:54 10.1.0.2 1,2016/11/15 0 8:46:54,001801015967,TRAFFIC ,start,1,2016/11/15 08:46:54 ,107.77.90.82,50.232.155.145 ,107.77.90.82,10.250.0.10,in bound-web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec ureworks,2016/11/15 08:46:54 ,20097,1,19717,80,19717,80,0 x400000,tcp,allow,727,653,74 ,4,2016/11/15 08:46:54,0,any ,0,2816307658,0x0,US,US,0,3, 1,n/a,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:46:55 10 .1.0.2 1,2016/11/15 08:46:55 ,001801015967,TRAFFIC,start, 1,2016/11/15 08:46:55,171.15 9.64.10,50.232.155.145,171.1 59.64.10,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:46:55,5486 1,1,10000,80,10000,80,0x4000 00,tcp,allow,597,523,74,4,20 16/11/15 08:46:55,0,any,0,28 16307729,0x0,US,US,0,3,1,n/a ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:46:55 10.1.0. 2 1,2016/11/15 08:46:55,0018 01015967,TRAFFIC,start,1,201 6/11/15 08:46:55,107.77.90.8 2,50.232.155.145,107.77.90.8 2,10.250.0.10,inbound-web-br owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201 6/11/15 08:46:55,41183,1,429 58,80,42958,80,0x400000,tcp, allow,569,495,74,4,2016/11/1 5 08:46:54,0,any,0,281630770 7,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:46:54 10.1.0.2 1,201 6/11/15 08:46:54,00180101596 7,TRAFFIC,end,1,2016/11/15 0 8:46:54,66.110.201.211,50.23 2.155.145,66.110.201.211,10. 250.0.10,inbound-web-browsin g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15 08:46:54,49541,1,62810,80 ,62810,80,0x40001a,tcp,allow ,17010,4069,12941,28,2016/11 /15 08:46:38,0,government,0, 2816307577,0x0,US,US,0,16,12 ,tcp-rst-from-client,0,0,0,0 ,,ATL-PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:46:54 10.1.0.2 1,2016 /11/15 08:46:54,001801015967 ,TRAFFIC,end,1,2016/11/15 08 :46:54,64.85.97.190,50.232.1 55.145,64.85.97.190,10.250.0 .10,inbound-web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15 08 :46:54,12683,1,53666,80,5366 6,80,0x40001c,tcp,allow,7476 9,9361,65408,118,2016/11/15 08:46:28,10,government,0,281 6307605,0x0,US,US,0,66,52,tc p-rst-from-client,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:46:53 10.1.0.2 1,2016/11 /15 08:46:53,001801015967,TR AFFIC,start,1,2016/11/15 08: 46:53,152.133.7.133,50.232.1 55.145,152.133.7.133,10.250. 0.10,inbound-web-browsing,,, web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0 8:46:53,35024,1,62758,80,627 58,80,0x400000,tcp,allow,160 6,1540,66,4,2016/11/15 08:46 :53,0,any,0,2816307553,0x0,U S,US,0,3,1,n/a,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :46:53 10.1.0.2 1,2016/11/15 08:46:53,001801015967,TRAFF IC,start,1,2016/11/15 08:46: 53,152.133.7.133,50.232.155. 145,152.133.7.133,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell - secureworks,2016/11/15 08:4 6:53,14146,1,41644,80,41644, 80,0x400000,tcp,allow,1606,1 540,66,4,2016/11/15 08:46:53 ,0,any,0,2816307546,0x0,US,U S,0,3,1,n/a,0,0,0,0,,ATL-PAN -01,from-policy
Nov 15 08:46 :53 10.1.0.2 1,2016/11/15 08 :46:53,001801015967,TRAFFIC, start,1,2016/11/15 08:46:53, 152.133.7.133,50.232.155.145 ,152.133.7.133,10.250.0.10,i nbound-web-browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15 08:46:5 3,19113,1,12667,80,12667,80, 0x400000,tcp,allow,1606,1540 ,66,4,2016/11/15 08:46:53,0, any,0,2816307548,0x0,US,US,0 ,3,1,n/a,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:46:53 10.1.0.2 1,2016/11/15 08:46 :53,001801015967,TRAFFIC,end ,1,2016/11/15 08:46:53,64.85 .77.7,50.232.155.145,64.85.7 7.7,10.250.0.10,inbound-web- browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2 016/11/15 08:46:53,43001,1,4 0898,80,40898,80,0x40001c,tc p,allow,82444,7208,75236,109 ,2016/11/15 08:45:18,79,gove rnment,0,2816307511,0x0,US,U S,0,53,56,tcp-fin,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:46:53 10.1.0.2 1,2016/11 /15 08:46:53,001801015967,TR AFFIC,start,1,2016/11/15 08: 46:53,152.133.7.133,50.232.1 55.145,152.133.7.133,10.250. 0.10,inbound-web-browsing,,, web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0 8:46:53,60660,1,33050,80,330 50,80,0x400000,tcp,allow,160 6,1540,66,4,2016/11/15 08:46 :53,0,any,0,2816307554,0x0,U S,US,0,3,1,n/a,0,0,0,0,,ATL- PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08 :46:53 10.1.0.2 1,2016/11/15 08:46:53,001801015967,TRAFF IC,end,1,2016/11/15 08:46:53 ,209.67.78.46,50.232.155.145 ,209.67.78.46,10.250.0.10,in bound-web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec ureworks,2016/11/15 08:46:53 ,43981,1,38385,80,38385,80,0 x40001c,tcp,allow,33376,2448 ,30928,50,2016/11/15 08:46:3 6,1,government,0,2816307517, 0x0,US,US,0,27,23,tcp-rst-fr om-client,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:46:5 2 10.1.0.2 1,2016/11/15 08:4 6:52,001801015967,TRAFFIC,en d,1,2016/11/15 08:46:52,209. 67.78.37,50.232.155.145,209. 67.78.37,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:46:52,4038 7,1,45572,80,45572,80,0x4000 1c,tcp,allow,2341,730,1611,9 ,2016/11/15 08:46:35,1,gover nment,0,2816307437,0x0,US,US ,0,6,3,tcp-rst-from-client,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:46:52 10.1.0.2 1,2016/11/15 08:46:52,001801 015967,TRAFFIC,start,1,2016/ 11/15 08:46:52,98.159.233.10 ,50.232.155.145,98.159.233.1 0,10.250.0.10,inbound-web-br owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201 6/11/15 08:46:52,59819,1,570 59,80,57059,80,0x400000,tcp, allow,681,607,74,4,2016/11/1 5 08:46:52,0,any,0,281630746 8,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:46:52 10.1.0.2 1,201 6/11/15 08:46:52,00180101596 7,TRAFFIC,start,1,2016/11/15 08:46:52,98.159.233.10,50.2 32.155.145,98.159.233.10,10. 250.0.10,inbound-web-browsin g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15 08:46:52,254121,1,57058,8 0,57058,80,0x400000,tcp,allo w,830,756,74,4,2016/11/15 08 :46:52,0,any,0,2816307467,0x 0,US,US,0,3,1,n/a,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:46:52 10.1.0.2 1,2016/11 /15 08:46:52,001801015967,TR AFFIC,start,1,2016/11/15 08: 46:52,98.159.233.10,50.232.1 55.145,98.159.233.10,10.250. 0.10,inbound-web-browsing,,, web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0 8:46:52,53221,1,57061,80,570 61,80,0x400000,tcp,allow,685 ,611,74,4,2016/11/15 08:46:5 2,0,any,0,2816307469,0x0,US, US,0,3,1,n/a,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 6:52 10.1.0.2 1,2016/11/15 0 8:46:52,001801015967,TRAFFIC ,end,1,2016/11/15 08:46:52,1 62.17.64.145,50.232.155.145, 162.17.64.145,10.250.0.10,in bound-web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec ureworks,2016/11/15 08:46:52 ,45010,1,49742,80,49742,80,0 x40001a,tcp,allow,32525,1740 ,30785,40,2016/11/15 08:46:3 2,4,government,0,2816307445, 0x0,US,US,0,16,24,tcp-rst-fr om-client,0,0,0,0,,ATL-PAN-0 1,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:46:5 1 10.1.0.2 1,2016/11/15 08:4 6:51,001801015967,TRAFFIC,en d,1,2016/11/15 08:46:51,152. 133.7.129,50.232.155.145,152 .133.7.129,10.250.0.10,inbou nd-web-browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure works,2016/11/15 08:46:51,57 199,1,4271,80,4271,80,0x4000 1a,tcp,allow,4266,2627,1639, 9,2016/11/15 08:46:35,0,gove rnment,0,2816307376,0x0,US,U S,0,5,4,tcp-rst-from-client, 0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:46:51 10.1.0.2 1,2016/11/15 08:46:51,00180 1015967,TRAFFIC,start,1,2016 /11/15 08:46:51,74.183.101.1 97,50.232.155.145,74.183.101 .197,10.250.0.10,inbound-web - browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15 08:46:51,46295,1, 53630,80,53630,80,0x400000,t cp,allow,565,491,74,4,2016/1 1/15 08:46:51,0,any,0,281630 7407,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:50 10.1.0.2 1, 2016/11/15 08:46:50,00180101 5967,TRAFFIC,start,1,2016/11 /15 08:46:50,74.183.101.197, 50.232.155.145,74.183.101.19 7,10.250.0.10,inbound-web-br owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201 6/11/15 08:46:50,47062,1,536 29,80,53629,80,0x400000,tcp, allow,729,655,74,4,2016/11/1 5 08:46:50,0,any,0,281630734 4,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:46:51 10.1.0.2 1,201 6/11/15 08:46:51,00180101596 7,TRAFFIC,end,1,2016/11/15 0 8:46:51,152.133.7.129,50.232 .155.145,152.133.7.129,10.25 0.0.10,inbound-web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15 08:46:51,250379,1,61701,80, 61701,80,0x40001a,tcp,allow, 4446,2747,1699,12,2016/11/15 08:45:51,44,government,0,28 16307360,0x0,US,US,0,7,5,tcp - rst-from-client,0,0,0,0,,AT L-PAN-01,from-policy
Nov 15 08:46:50 10.1.0.2 1,2016/11/ 15 08:46:50,001801015967,TRA FFIC,start,1,2016/11/15 08:4 6:50,64.85.97.203,50.232.155 .145,64.85.97.203,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell - secureworks,2016/11/15 08:4 6:50,48057,1,46679,80,46679, 80,0x400000,tcp,allow,684,61 0,74,4,2016/11/15 08:46:50,0 ,any,0,2816307345,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:46:5 1 10.1.0.2 1,2016/11/15 08:4 6:51,001801015967,TRAFFIC,en d,1,2016/11/15 08:46:51,209. 67.78.45,50.232.155.145,209. 67.78.45,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:46:51,4652 7,1,50501,80,50501,80,0x4000 1c,tcp,allow,168312,21752,14 6560,239,2016/11/15 08:45:19 ,76,government,0,2816307392, 0x0,US,US,0,125,114,tcp-rst-from-client,0,0,0,0,,ATL-PAN -01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:46 :50 10.1.0.2 1,2016/11/15 08 :46:50,001801015967,TRAFFIC, end,1,2016/11/15 08:46:50,47 .32.70.122,50.232.155.145,47 .32.70.122,10.250.0.10,inbou nd-web-browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure works,2016/11/15 08:46:50,29 061,1,54717,80,54717,80,0x40 001a,tcp,allow,48519,3706,44 813,49,2016/11/15 08:46:29,5 ,government,0,2816307312,0x0 ,US,US,0,17,32,tcp-rst-from-client,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:46:49 1 0.1.0.2 1,2016/11/15 08:46:4 9,001801015967,TRAFFIC,start ,1,2016/11/15 08:46:49,64.85 .77.10,50.232.155.145,64.85. 77.10,10.250.0.10,inbound-we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-secureworks ,2016/11/15 08:46:49,44233,1 ,43157,80,43157,80,0x400000, tcp,allow,684,610,74,4,2016/ 11/15 08:46:49,0,any,0,28163 07244,0x0,US,US,0,3,1,n/a,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:46:50 10.1.0.2 1 ,2016/11/15 08:46:50,0018010 15967,TRAFFIC,start,1,2016/1 1/15 08:46:50,64.85.77.13,50 .232.155.145,64.85.77.13,10. 250.0.10,inbound-web-browsin g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15 08:46:50,43987,1,60433,80 ,60433,80,0x400000,tcp,allow ,703,629,74,4,2016/11/15 08: 46:49,0,any,0,2816307328,0x0 ,US,US,0,3,1,n/a,0,0,0,0,,AT L-PAN-01,from-policy
Nov 15 08:46:50 10.1.0.2 1,2016/11/ 15 08:46:50,001801015967,TRA FFIC,end,1,2016/11/15 08:46: 50,47.32.70.122,50.232.155.1 45,47.32.70.122,10.250.0.10, inbound-web-browsing,,,web-b rowsing,vsys1,outside,dmz,et hernet1/4,ethernet1/2,dell-s ecureworks,2016/11/15 08:46: 50,22070,1,54720,80,54720,80 ,0x40001a,tcp,allow,2059,534 ,1525,7,2016/11/15 08:46:29, 5,government,0,2816307283,0x 0,US,US,0,5,2,tcp-rst-from-c lient,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:46:49 10 .1.0.2 1,2016/11/15 08:46:49 ,001801015967,TRAFFIC,end,1, 2016/11/15 08:46:49,209.67.7 8.56,50.232.155.145,209.67.7 8.56,10.250.0.10,inbound-web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15 08:46:49,15858,1, 37151,80,37151,80,0x40001c,t cp,allow,4792,2353,2439,18,2 016/11/15 08:46:31,2,governm ent,0,2816307202,0x0,US,US,0 ,12,6,tcp-rst-from-client,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:46:49 10.1.0.2 1 ,2016/11/15 08:46:49,0018010 15967,TRAFFIC,end,1,2016/11/ 15 08:46:49,12.48.151.106,50 .232.155.145,12.48.151.106,1 0.250.0.10,inbound-web-brows ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15 08:46:49,26931,1,26119, 80,26119,80,0x40001c,tcp,all ow,2808,809,1999,16,2016/11/ 15

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

08:46:14,19,government,0, 2816307196,0x0,US,US,0,6,10, tcp-rst-from-client,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:46:49 10.1.0.2 1,2016/ 11/15 08:46:49,001801015967, TRAFFIC,end,1,2016/11/15 08: 46:49,64.179.192.42,50.232.1 55.145,64.179.192.42,10.250. 0.10,inbound-web-browsing,,, web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0 8:46:49,22828,1,41856,80,418 56,80,0x40001a,tcp,allow,272 2,1197,1525,7,2016/11/15 08: 46:32,1,government,0,2816307 207,0x0,US,US,0,5,2,tcp-rst- from-client,0,0,0,0,,ATL-PAN -01,from-policy
Nov 15 08:46 :49 10.1.0.2 1,2016/11/15 08 :46:49,001801015967,TRAFFIC, end,1,2016/11/15 08:46:49,15 2.133.7.129,50.232.155.145,1 52.133.7.129,10.250.0.10,inb ound-web-browsing,,,web-brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu reworks,2016/11/15 08:46:49, 42821,1,24166,80,24166,80,0x 40001a,tcp,allow,56012,16287 ,39725,64,2016/11/15 08:46:2 2,11,government,0,2816307195 ,0x0,US,US,0,28,36,tcp-rst-f rom-client,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46: 49 10.1.0.2 1,2016/11/15 08: 46:49,001801015967,TRAFFIC,s tart,1,2016/11/15 08:46:49,6 4.85.97.253,50.232.155.145,6 4.85.97.253,10.250.0.10,inbo und-web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:46:49,3 2082,1,45056,80,45056,80,0x4 00000,tcp,allow,603,529,74,4 ,2016/11/15 08:46:48,0,any,0 ,2816307193,0x0,US,US,0,3,1, n/ a,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:46:48 10.1 .0.2 1,2016/11/15 08:46:48,0 01801015967,TRAFFIC,end,1,20 16/11/15 08:46:48,64.85.77.1 3,50.232.155.145,64.85.77.13 ,10.250.0.10,inbound-web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:46:48,37215,1,3480 8,80,34808,80,0x40001c,tcp,a llow,49684,10931,38753,72,20 16/11/15 08:46:22,10,governm ent,0,2816307144,0x0,US,US,0 ,40,32,tcp-fin,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :46:48 10.1.0.2 1,2016/11/15 08:46:48,001801015967,TRAFF IC,end,1,2016/11/15 08:46:48 ,158.111.236.10,50.232.155.1 45,158.111.236.10,10.250.0.1 0,inbound-web-browsing,,,web - browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4 6:48,262107,1,40201,80,40201 ,80,0x40001a,tcp,allow,77791 ,4895,72896,80,2016/11/15 08 :46:14,18,government,0,28163 07142,0x0,US,US,0,26,54,tcp- rst-from-client,0,0,0,0,,ATL - PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 0 8:46:47 10.1.0.2 1,2016/11/1 5 08:46:47,001801015967,TRAF FIC,end,1,2016/11/15 08:46:4 7,205.173.105.205,50.232.155 .145,205.173.105.205,10.250. 0.10,inbound-web-browsing,,, web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0 8:46:47,33789,1,32259,80,322 59,80,0x40001a,tcp,allow,225 1,672,1579,7,2016/11/15 08:4 6:31,0,government,0,28163070 46,0x0,US,US,0,4,3,tcp-rst-f rom-client,0,0,0,0,,ATL-PAN- 01,from-policy
Nov 15 08:46: 47 10.1.0.2 1,2016/11/15 08: 46:47,001801015967,TRAFFIC,e nd,1,2016/11/15 08:46:47,205 .173.105.205,50.232.155.145, 205.173.105.205,10.250.0.10, inbound-web-browsing,,,web-b rowsing,vsys1,outside,dmz,et hernet1/4,ethernet1/2,dell-s ecureworks,2016/11/15 08:46: 47,38380,1,33247,80,33247,80 ,0x40001a,tcp,allow,2104,525 ,1579,8,2016/11/15 08:46:31, 0,government,0,2816307051,0x 0,US,US,0,5,3,tcp-rst-from-c lient,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:46:46 10 .1.0.2 1,2016/11/15 08:46:46 ,001801015967,TRAFFIC,end,1, 2016/11/15 08:46:46,108.226. 66.78,50.232.155.145,108.226 .66.78,10.250.0.10,inbound-w eb-browsing,,,web-browsing,v sys1,outside,dmz,ethernet1/4 ,ethernet1/2,dell-securework s,2016/11/15 08:46:46,56375, 1,56709,80,56709,80,0x40001a ,tcp,allow,49511,8171,41340, 56,2016/11/15 08:46:13,17,go vernment,0,2816306989,0x0,US ,US,0,24,32,tcp-rst-from-cli ent,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:46:46 10.1 .0.2 1,2016/11/15 08:46:46,0 01801015967,TRAFFIC,end,1,20 16/11/15 08:46:46,66.192.63. 2,50.232.155.145,66.192.63.2 ,10.250.0.10,inbound-web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:46:46,46741,1,5445 7,80,54457,80,0x40001c,tcp,a llow,75951,16926,59025,68,20 16/11/15 08:45:23,67,governm ent,0,2816306994,0x0,US,US,0 ,25,43,tcp-fin,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :46:45 10.1.0.2 1,2016/11/15 08:46:45,001801015967,TRAFF IC,end,1,2016/11/15 08:46:45 ,47.32.70.122,50.232.155.145 ,47.32.70.122,10.250.0.10,in bound-web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec ureworks,2016/11/15 08:46:45 ,40902,1,54721,80,54721,80,0 x40001a,tcp,allow,2059,534,1 525,7,2016/11/15 08:46:29,0, government,0,2816306863,0x0, US,US,0,5,2,tcp-rst-from-cli ent,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:46:45 10.1 .0.2 1,2016/11/15 08:46:45,0 01801015967,TRAFFIC,end,1,20 16/11/15 08:46:45,66.110.201 .211,50.232.155.145,66.110.2 01.211,10.250.0.10,inbound-w eb-browsing,,,web-browsing,v

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

sys1,outside,dmz,ethernet1/4 ,ethernet1/2,dell-securework s,2016/11/15 08:46:45,46896,
1,62804,80,62804,80,0x40001a ,tcp,allow,85669,16478,69191 ,108,2016/11/15 08:46:19,10,
government,0,2816306936,0x0, US,US,0,56,52,tcp-rst-from-c lient,0,0,0,0,,ATL-PAN-01,fr om-
policy
Nov 15 08:46:45 10 .1.0.2 1,2016/11/15 08:46:45 ,001801015967,TRAFFIC,end,1,
2016/11/15 08:46:45,47.32.70 .122,50.232.155.145,47.32.70 .122,10.250.0.10,inbound-web
-browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks,
2016/11/15 08:46:45,53754,1, 54716,80,54716,80,0x40001a,t cp,allow,5788,2162,3626,10,2
016/11/15 08:46:29,0,governm ent,0,2816306858,0x0,US,US,0 ,6,4,tcp-rst-from-
client,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:44 10.1.0.2 1, 2016/11/15 08:46:44,00180101 5967,TRAFFIC,end,1,2016/11/1
5 08:46:44,64.85.97.227,50.2 32.155.145,64.85.97.227,10.2 50.0.10,inbound-
web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-
secureworks,2016/11/1 5 08:46:44,52889,1,35803,80, 35803,80,0x40001c,tcp,allow,
39528,8206,31322,56,2016/11/ 15 08:46:27,1,government,0,2 816306825,0x0,US,US,0,31,25,
tcp-rst-from-client,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:46:43 10.1.0.2 1,2016/ 11/15 08:46:43,001801015967, TRAFFIC,end,1,2016/11/15
08: 46:43,162.41.8.10,50.232.155 .145,162.41.8.10,10.250.0.10 ,inbound-web-browsing,,,inco
mplete,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15 08:46:4
3,14965,1,54683,80,54683,80, 0x40001b,tcp,allow,340,206,1 34,5,2016/11/15 08:45:17,70,
any,0,2816306783,0x0,US,US,0 ,3,2,tcp-rst-from-server,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:43 10.1.0.2 1, 2016/11/15 08:46:43,00180101 5967,TRAFFIC,end,1,2016/11/1
5 08:46:43,209.67.78.58,50.2 32.155.145,209.67.78.58,10.2 50.0.10,inbound-
web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/
2,dell-secureworks,2016/11/1 5 08:46:43,42022,1,39192,80,
39192,80,0x40001c,tcp,allow, 104939,14890,90049,153,2016/ 11/15
08:46:17,10,government ,0,2816306744,0x0,US,US,0,82 ,71,tcp-rst-from-client,0,0, 0,0,,ATL-
PAN-01,from-policy
Nov 15 08:46:43 10.1.0.2 1,2 016/11/15 08:46:43,001801015 967,TRAFFIC,end,1,2016/11/15
08:46:43,64.85.77.9,50.232. 155.145,64.85.77.9,10.250.0. 10,inbound-web-browsing,,,we
b-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08:
46:43,26074,1,48165,80,48165 ,80,0x40001c,tcp,allow,31051 ,1594,29457,41,2016/11/15
08 :45:27,60,government,0,28163 06756,0x0,US,US,0,19,22,tcp- fin,0,0,0,0,,ATL-PAN-01,from
-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:46:43 10.1 .0.2 1,2016/11/15 08:46:43,0 01801015967,TRAFFIC,end,1,20 16/11/15 08:46:43,162.41.8.1 0,50.232.155.145,162.41.8.10 ,10.250.0.10,inbound-web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:46:43,40973,1,1124 4,80,11244,80,0x40001c,tcp,a llow,2417,740,1677,10,2016/1 1/15 08:45:17,70,government, 0,2816306758,0x0,US,US,0,6,4 ,tcp-fin,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:46:43 10.1.0.2 1,2016/11/15 08:46 :43,001801015967,TRAFFIC,end ,1,2016/11/15 08:46:43,64.85 .97.207,50.232.155.145,64.85 .97.207,10.250.0.10,inbound-web-browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-securewor ks,2016/11/15 08:46:43,46220 ,1,53938,80,53938,80,0x40001 c,tcp,allow,33870,3465,30405 ,55,2016/11/15 08:46:15,12,g overnment,0,2816306739,0x0,U S,US,0,30,25,tcp-fin,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:46:42 10.1.0.2 1,2016 /11/15 08:46:42,001801015967 ,TRAFFIC,start,1,2016/11/15 08:46:42,47.32.70.122,50.232 .155.145,47.32.70.122,10.250 .0.10,inbound-web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15 08:46:42,39270,1,54722,80,54 722,80,0x400000,tcp,allow,11 81,1115,66,4,2016/11/15 08:4 6:40,1,any,0,2816306645,0x0, US,US,0,3,1,n/a,0,0,0,0,,ATL - PAN-01,from-policy
Nov 15 0 8:46:42 10.1.0.2 1,2016/11/1 5 08:46:42,001801015967,TRAF FIC,end,1,2016/11/15 08:46:4 2,12.206.16.210,50.232.155.1 45,12.206.16.210,10.250.0.10 ,inbound-web-browsing,,,inco mplete,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15 08:46:4 2,52691,1,52452,80,52452,80, 0x40001b,tcp,allow,312,186,1 26,5,2016/11/15 08:46:21,5,a ny,0,2816306663,0x0,US,US,0, 3,2,tcp-rst-from-server,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:41 10.1.0.2 1,2 016/11/15 08:46:41,001801015 967,TRAFFIC,start,1,2016/11/ 15 08:46:41,209.67.78.36,50. 232.155.145,209.67.78.36,10. 250.0.10,inbound-web-browsin g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15 08:46:41,15720,1,50013,80 ,50013,80,0x400000,tcp,allow ,693,619,74,4,2016/11/15 08: 46:40,0,any,0,2816306631,0x0 ,US,US,0,3,1,n/a,0,0,0,0,,AT L-PAN-01,from-policy
Nov 15 08:46:40 10.1.0.2 1,2016/11/ 15 08:46:40,001801015967,TRA FFIC,end,1,2016/11/15 08:46: 40,64.85.77.6,50.232.155.145 ,64.85.77.6,10.250.0.10,inbo und-web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:46:40,3 8398,1,48920,80,48920,80,0x4 0001c,tcp,allow,3166,1279,18 87,12,2016/11/15

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

08:45:19,65 ,government,0,2816306550,0x0 ,US,US,0,8,4,tcp-fin,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:46:40 10.1.0.2 1,2016 /11/15 08:46:40,001801015967 ,TRAFFIC,end,1,2016/11/15 08 :46:40,74.174.56.6,50.232.15 5.145,74.174.56.6,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4 6:40,42179,1,63726,80,63726, 80,0x40001a,tcp,allow,2926,1 287,1639,10,2016/11/15 08:46 :24,0,government,0,281630652 2,0x0,US,US,0,6,4,tcp-rst-fr om-client,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:46:4 0 10.1.0.2 1,2016/11/15 08:4 6:40,001801015967,TRAFFIC,en d,1,2016/11/15 08:46:40,64.8 5.97.180,50.232.155.145,64.8 5.97.180,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:46:40,2631 3,1,51694,80,51694,80,0x4000 1c,tcp,allow,35497,4597,3090 0,59,2016/11/15 08:46:16,8,g overnment,0,2816306538,0x0,U S,US,0,33,26,tcp-rst-from-cl ient,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:46:40 10. 1.0.2 1,2016/11/15 08:46:40, 001801015967,TRAFFIC,end,1,2 016/11/15 08:46:40,74.174.56 .6,50.232.155.145,74.174.56. 6,10.250.0.10,inbound-web-br owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201 6/11/15 08:46:40,54281,1,119 92,80,11992,80,0x40001a,tcp, allow,2746,1167,1579,7,2016/ 11/15 08:46:24,0,government, 0,2816306530,0x0,US,US,0,4,3 ,tcp-rst-from-client,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:46:39 10.1.0.2 1,2016 /11/15 08:46:39,001801015967 ,TRAFFIC,start,1,2016/11/15 08:46:39,64.85.97.176,50.232 .155.145,64.85.97.176,10.250 .0.10,inbound-web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15 08:46:39,46645,1,52855,80,52 855,80,0x400000,tcp,allow,61 7,543,74,4,2016/11/15 08:46: 38,1,any,0,2816306494,0x0,US ,US,0,3,1,n/a,0,0,0,0,,ATL-P AN-01,from-policy
Nov 15 08: 46:39 10.1.0.2 1,2016/11/15 08:46:39,001801015967,TRAFFI C,start,1,2016/11/15 08:46:3 9,209.67.78.50,50.232.155.14 5,209.67.78.50,10.250.0.10,i nbound-web-browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15 08:46:3 9,72621,1,33411,80,33411,80, 0x400000,tcp,allow,600,526,7 4,4,2016/11/15 08:46:39,0,an y,0,2816306501,0x0,US,US,0,3 ,1,n/a,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:46:39 1 0.1.0.2 1,2016/11/15 08:46:3 9,001801015967,TRAFFIC,start ,1,2016/11/15 08:46:39,66.11 0.201.211,50.232.155.145,66. 110.201.211,10.250.0.10,inbo und-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-
secur eworks,2016/11/15 08:46:39,2 6783,1,62811,80,62811,80,0x4
00000,tcp,allow,1728,1654,74 ,4,2016/11/15 08:46:38,0,any ,0,2816306491,0x0,US,US,0,3,
1,n/a,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:46:39 10 .1.0.2 1,2016/11/15 08:46:39 ,001801015967,TRAFFIC,end,1, 2016/11/15
08:46:39,70.133.2 22.130,50.232.155.145,70.133 .222.130,10.250.0.10,inbound -web-
browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo
rks,2016/11/15 08:46:39,4706 7,1,61085,80,61085,80,0x4000 1c,tcp,allow,65032,4796,6023
6,86,2016/11/15 08:46:20,3,g overnment,0,2816306464,0x0,U S,US,0,41,45,tcp-
fin,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:46:38 10.1.0.2 1,2016 /11/15 08:46:38,001801015967 ,TRAFFIC,end,1,2016/11/15
08 :46:38,174.218.130.192,50.23 2.155.145,174.218.130.192,10 .250.0.10,inbound-web-browsi
ng,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15
08:46:38,47675,1,7198,80 ,7198,80,0x40001c,tcp,allow, 33853,2719,31134,54,2016/11/ 15
08:46:20,2,government,0,2 816306418,0x0,US,US,0,29,25, tcp-fin,0,0,0,0,,ATL-PAN-01, from-
policy
Nov 15 08:46:38 10.1.0.2 1,2016/11/15 08:46: 38,001801015967,TRAFFIC,end, 1,2016/11/15
08:46:38,64.85. 77.13,50.232.155.145,64.85.7 7.13,10.250.0.10,inbound-web -browsing,,,web-
browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15
08:46:38,44150,1, 44945,80,44945,80,0x40001c,t cp,allow,2094,1282,812,12,20 16/11/15
08:46:20,2,governme nt,0,2816306362,0x0,US,US,0, 8,4,tcp-fin,0,0,0,0,,ATL-PAN -01,from-
policy
Nov 15 08:46 :38 10.1.0.2 1,2016/11/15 08 :46:38,001801015967,TRAFFIC, end,1,2016/11/15
08:46:38,17 4.218.130.192,50.232.155.145 ,174.218.130.192,10.250.0.10 ,inbound-
web-browsing,,,web- browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell-
secureworks,2016/11/15 08:46 :38,53633,1,7195,80,7195,80,
0x40001c,tcp,allow,4044,1464 ,2580,14,2016/11/15 08:46:20 ,2,government,0,2816306396,0
x0,US,US,0,9,5,tcp-fin,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:46:38 10.1.0.2 1,20 16/11/15 08:46:38,0018010159 67,TRAFFIC,start,1,2016/11/1
5 08:46:38,158.111.236.10,50 .232.155.145,158.111.236.10, 10.250.0.10,inbound-web-brow
sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/
11/15 08:46:38,45758,1,28219 ,80,28219,80,0x400000,tcp,al low,794,732,62,4,2016/11/15
08:46:38,0,any,0,2816306436, 0x0,US,US,0,3,1,n/a,0,0,0,0, ,ATL-PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:46:38 10.1.0.2 1,2016/ 11/15 08:46:38,001801015967, TRAFFIC,end,1,2016/11/15 08: 46:38,174.218.130.192,50.232 .155.145,174.218.130.192,10. 250.0.10,inbound-web-browsin g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15 08:46:38,46644,1,7181,80, 7181,80,0x40001c,tcp,allow,1 5813,1416,14397,27,2016/11/1 5 08:46:21,1,government,0,28 16306366,0x0,US,US,0,15,12,t cp-fin,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:46:38 1 0.1.0.2 1,2016/11/15 08:46:3 8,001801015967,TRAFFIC,start ,1,2016/11/15 08:46:38,158.1 11.236.10,50.232.155.145,158 .111.236.10,10.250.0.10,inbo und-web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:46:38,4 3178,1,38695,80,38695,80,0x4 00000,tcp,allow,859,797,62,4 ,2016/11/15 08:46:38,0,any,0 ,2816306429,0x0,US,US,0,3,1, n/a,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:46:38 10.1 .0.2 1,2016/11/15 08:46:38,0 01801015967,TRAFFIC,start,1, 2016/11/15 08:46:38,66.110.2 01.211,50.232.155.145,66.110 .201.211,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:46:38,4954 1,1,62810,80,62810,80,0x4000 00,tcp,allow,1728,1654,74,4, 2016/11/15 08:46:38,0,any,0, 2816306431,0x0,US,US,0,3,1,n /a,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:38 10.1. 0.2 1,2016/11/15 08:46:38,00 1801015967,TRAFFIC,end,1,201 6/11/15 08:46:38,158.111.236 .10,50.232.155.145,158.111.2 36.10,10.250.0.10,inbound-we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-secureworks ,2016/11/15 08:46:38,51862,1 ,38665,80,38665,80,0x40001a, tcp,allow,56070,8821,47249,5 6,2016/11/15 08:46:14,8,gove rnment,0,2816306374,0x0,US,U S,0,20,36,tcp-rst-from-clien t,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:46:37 10.1.0 .2 1,2016/11/15 08:46:37,001 801015967,TRAFFIC,start,1,20 16/11/15 08:46:37,64.85.77.2 ,50.232.155.145,64.85.77.2,1 0.250.0.10,inbound-web-brows ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15 08:46:37,54728,1,60734, 80,60734,80,0x400000,tcp,all ow,684,610,74,4,2016/11/15 0 8:46:37,0,any,0,2816306316,0 x0,US,US,0,3,1,n/a,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:46:37 10.1.0.2 1,2016/1 1/15 08:46:37,001801015967,T RAFFIC,drop,1,2016/11/15 08: 46:37,27.74.136.239,50.232.1 55.145,0.0.0.0,0.0.0.0,deny- remaining,,,not-applicable,v sys1,outside,dmz,ethernet1/4 ,,dell-secureworks,2016/11/1 5 08:46:37,0,1,43784,23,0,0, 0x0,tcp,deny,60,60,0,1,2016/ 11/15 08:46:37,0,any,0,28163 06324,0x0,VN,US,0,1,0,policy -deny,0,0,0,0,,ATL-PAN-01,fr om-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:46:37 10 .1.0.2 1,2016/11/15 08:46:37 ,001801015967,TRAFFIC,start, 1,2016/11/15 08:46:37,174.21 8.133.21,50.232.155.145,174. 218.133.21,10.250.0.10,inbou nd-web-browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure works,2016/11/15 08:46:37,48 359,1,10491,80,10491,80,0x40 0000,tcp,allow,520,446,74,4, 2016/11/15 08:46:37,0,any,0, 2816306312,0x0,US,US,0,3,1,n /a,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:37 10.1. 0.2 1,2016/11/15 08:46:37,00 1801015967,TRAFFIC,start,1,2 016/11/15 08:46:37,174.218.1 33.21,50.232.155.145,174.218 .133.21,10.250.0.10,inbound-web-browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-secureworks,2016/11/15 08:46:37,49120 ,1,2529,80,2529,80,0x400000, tcp,allow,678,604,74,4,2016/11/15 08:46:36,0,any,0,28163 06279,0x0,US,US,0,3,1,n/a,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:46:37 10.1.0.2 1 ,2016/11/15 08:46:37,0018010 15967,TRAFFIC,end,1,2016/11/15 08:46:37,207.99.81.78,50. 232.155.145,207.99.81.78,10. 250.0.10,inbound-web-browsing,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15 08:46:37,37563,1,2620,80, 2620,80,0x40001a,tcp,allow,3 0598,3530,27068,41,2016/11/1 5 08:45:58,23,government,0,2 816306297,0x0,US,US,0,16,25, tcp-rst-from-client,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:46:37 10.1.0.2 1,2016/ 11/15 08:46:37,001801015967, TRAFFIC,end,1,2016/11/15 08: 46:37,74.174.56.6,50.232.155 .145,74.174.56.6,10.250.0.10 ,inbound-web-browsing,,,web-browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell- secureworks,2016/11/15 08:46 :37,45125,1,11383,80,11383,8 0,0x40001a,tcp,allow,4049,22 06,1843,10,2016/11/15 08:46: 17,4,government,0,2816306303 ,0x0,US,US,0,6,4,tcp-rst-fro m-client,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:46:37 10.1.0.2 1,2016/11/15 08:46 :37,001801015967,TRAFFIC,end ,1,2016/11/15 08:46:37,152.1 33.7.129,50.232.155.145,152. 133.7.129,10.250.0.10,inboun d-web-browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew orks,2016/11/15 08:46:37,357 09,1,61699,80,61699,80,0x400 01a,tcp,allow,3157,3031,126, 8,2016/11/15 08:45:51,30,gov ernment,0,2816306281,0x0,US, US,0,6,2,tcp-rst-from-client ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:46:36 10.1.0. 2 1,2016/11/15 08:46:36,0018 01015967,TRAFFIC,start,1,201 6/11/15 08:46:36,152.133.7.1 29,50.232.155.145,152.133.7. 129,10.250.0.10,inbound-web- browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2 016/11/15 08:46:36,250379,1, 61701,80,61701,80,0x400000,t

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

cp,allow,1606,1540,66,4,2016 /11/15 08:45:51,44,any,0,281 6306214,0x0,US,US,0,3,1,n/a,
0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:46:36 10.1.0.2 1,2016/11/15 08:46:36,00180 1015967,TRAFFIC,start,1,2016 /11/15
08:46:36,152.133.7.12 9,50.232.155.145,152.133.7.1 29,10.250.0.10,inbound-web-b
rowsing,,,web-browsing,vsys1 ,outside,dmz,ethernet1/4,eth ernet1/2,dell-secureworks,20
16/11/15 08:46:36,57199,1,42 71,80,4271,80,0x400000,tcp,a llow,1606,1540,66,4,2016/11/ 15
08:46:35,0,any,0,28163062 50,0x0,US,US,0,3,1,n/a,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:46:36 10.1.0.2 1,20 16/11/15 08:46:36,0018010159 67,TRAFFIC,start,1,2016/11/1
5 08:46:36,209.67.78.37,50.2 32.155.145,209.67.78.37,10.2 50.0.10,inbound-
web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-
secureworks,2016/11/1 5 08:46:36,40387,1,45572,80, 45572,80,0x400000,tcp,allow,
618,544,74,4,2016/11/15 08:4 6:35,0,any,0,2816306253,0x0, US,US,0,3,1,n/a,0,0,0,0,,ATL -
PAN-01,from-policy
Nov 15 0 8:46:36 10.1.0.2 1,2016/11/1 5 08:46:36,001801015967,TRAF FIC,start,1,2016/11/15
08:46 :36,66.192.63.2,50.232.155.1 45,66.192.63.2,10.250.0.10,i nbound-web-browsing,,,web-
br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15 08:46:3
6,55348,1,59229,80,59229,80, 0x400000,tcp,allow,1523,1449 ,74,4,2016/11/15 08:46:35,0,
any,0,2816306198,0x0,US,US,0 ,3,1,n/a,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:46:36 10.1.0.2 1,2016/11/15 08:46 :36,001801015967,TRAFFIC,sta rt,1,2016/11/15
08:46:36,209 .67.78.46,50.232.155.145,209 .67.78.46,10.250.0.10,inboun d-web-
browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew
orks,2016/11/15 08:46:36,439 81,1,38385,80,38385,80,0x400 000,tcp,allow,612,538,74,4,2
016/11/15 08:46:36,0,any,0,2 816306274,0x0,US,US,0,3,1,n/ a,0,0,0,0,,ATL-PAN-01,from-p
olicy
Nov 15 08:46:36 10.1.0 .2 1,2016/11/15 08:46:35,001 801015967,TRAFFIC,start,1,20
16/11/15 08:46:35,152.133.7. 129,50.232.155.145,152.133.7 .129,10.250.0.10,inbound-
web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-
secureworks, 2016/11/15 08:46:35,45581,1, 61700,80,61700,80,0x400000,t
cp,allow,1606,1540,66,4,2016 /11/15 08:45:51,44,any,0,281 6306192,0x0,US,US,0,3,1,n/a,
0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:46:35 10.1.0.2 1,2016/11/15 08:46:35,00180 1015967,TRAFFIC,end,1,2016/1
1/15 08:46:35,12.206.16.210, 50.232.155.145,12.206.16.210 ,10.250.0.10,inbound-
web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-
secureworks,2016 /11/15 08:46:35,50726,1,5244 5,80,52445,80,0x40001c,tcp,a

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

llow,78627,14613,64014,105,2 016/11/15 08:45:57,22,govern ment,0,2816306185,0x0,US,US,
0,44,61,tcp-rst-from-client, 0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:46:35 10.1.0.2 1,2016/11/15 08:46:35,00180 1015967,TRAFFIC,end,1,2016/1
1/15 08:46:35,64.85.77.10,50 .232.155.145,64.85.77.10,10. 250.0.10,inbound-web-browsin
g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15
08:46:35,31837,1,52268,80 ,52268,80,0x40001c,tcp,allow ,1243,827,416,9,2016/11/15 0
8:45:19,60,government,0,2816 306168,0x0,US,US,0,6,3,tcp-f in,0,0,0,0,,ATL-PAN-01,from-
policy
Nov 15 08:46:35 10.1. 0.2 1,2016/11/15 08:46:35,00 1801015967,TRAFFIC,end,1,201
6/11/15 08:46:35,66.110.201. 211,50.232.155.145,66.110.20 1.211,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-
secureworks ,2016/11/15 08:46:35,23337,1 ,62684,80,62684,80,0x40001a,
tcp,allow,156260,29800,12646 0,198,2016/11/15 08:43:27,17 2,government,0,2816306187,0x
0,US,US,0,106,92,tcp-rst-fro m-client,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:46:34 10.1.0.2 1,2016/11/15 08:46 :34,001801015967,TRAFFIC,sta rt,1,2016/11/15
08:46:34,47. 32.70.122,50.232.155.145,47. 32.70.122,10.250.0.10,inboun d-web-
browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew
orks,2016/11/15 08:46:34,220 70,1,54720,80,54720,80,0x400 000,tcp,allow,480,414,66,4,2
016/11/15 08:46:29,5,any,0,2 816306146,0x0,US,US,0,3,1,n/ a,0,0,0,0,,ATL-PAN-01,from-p
olicy
Nov 15 08:46:34 10.1.0 .2 1,2016/11/15 08:46:34,001 801015967,TRAFFIC,end,1,2016 /11/15
08:46:34,64.85.77.2,5 0.232.155.145,64.85.77.2,10. 250.0.10,inbound-web-browsin g,,,web-
browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15
08:46:34,39087,1,60073,80 ,60073,80,0x40001c,tcp,allow ,37219,7435,29784,47,2016/11 /15
08:45:17,61,government,0 ,2816306131,0x0,US,US,0,24,2 3,tcp-fin,0,0,0,0,,ATL-PAN-0 1,from-
policy
Nov 15 08:46:3 4 10.1.0.2 1,2016/11/15 08:4 6:34,001801015967,TRAFFIC,en d,1,2016/11/15
08:46:34,64.8 5.77.4,50.232.155.145,64.85. 77.4,10.250.0.10,inbound-web -browsing,,,web-
browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15
08:46:34,55410,1, 36032,80,36032,80,0x40001c,t cp,allow,5062,1705,3357,15,2 016/11/15
08:46:11,7,governm ent,0,2816306136,0x0,US,US,0 ,10,5,tcp-rst-from-client,0, 0,0,0,,ATL-
PAN-01,from-polic y
Nov 15 08:46:33 10.1.0.2 1 ,2016/11/15 08:46:33,0018010 15967,TRAFFIC,start,1,2016/1
1/15 08:46:33,162.17.64.145, 50.232.155.145,162.17.64.145 ,10.250.0.10,inbound-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:46:33,45010,1,4974 2,80,49742,80,0x400000,tcp,a llow,574,508,66,4,2016/11/15 08:46:32,0,any,0,2816306027 ,0x0,US,US,0,3,1,n/ a,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:46:33 10.1.0.2 1,2016 /11/15 08:46:33,001801015967 ,TRAFFIC,start,1,2016/11/15 08:46:33,64.179.192.42,50.23 2.155.145,64.179.192.42,10.2 50.0.10,inbound-web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5 08:46:33,22828,1,41856,80, 41856,80,0x400000,tcp,allow, 1143,1077,66,4,2016/11/15 08 :46:32,1,any,0,2816306065,0x 0,US,US,0,3,1,n/a,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:46:33 10.1.0.2 1,2016/11 /15 08:46:33,001801015967,TR AFFIC,end,1,2016/11/15 08:46 :33,209.67.78.51,50.232.155. 145,209.67.78.51,10.250.0.10 ,inbound-web-browsing,,,web- browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell-secureworks,2016/11/15 08:46 :33,53728,1,36716,80,36716,8 0,0x40001c,tcp,allow,141603, 18583,123020,206,2016/11/15 08:46:00,17,government,0,281 6306039,0x0,US,US,0,110,96,t cp-fin,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:46:33 1 0.1.0.2 1,2016/11/15 08:46:3 3,001801015967,TRAFFIC,start ,1,2016/11/15 08:46:33,162.1 7.64.145,50.232.155.145,162. 17.64.145,10.250.0.10,inboun d-web-browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew orks,2016/11/15 08:46:33,596 31,1,49743,80,49743,80,0x400 000,tcp,allow,671,605,66,4,2 016/11/15 08:46:32,0,any,0,2 816306029,0x0,US,US,0,3,1,n/ a,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:46:33 10.1.0 .2 1,2016/11/15 08:46:33,001 801015967,TRAFFIC,start,1,20 16/11/15 08:46:33,162.17.64. 145,50.232.155.145,162.17.64 .145,10.250.0.10,inbound-web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15 08:46:33,37046,1, 49744,80,49744,80,0x400000,t cp,allow,697,631,66,4,2016/1 1/15 08:46:32,0,any,0,281630 6063,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:33 10.1.0.2 1, 2016/11/15 08:46:33,00180101 5967,TRAFFIC,start,1,2016/11 /15 08:46:33,162.17.64.145,5 0.232.155.145,162.17.64.145, 10.250.0.10,inbound-web-brow sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/ 11/15 08:46:33,16856,1,49745 ,80,49745,80,0x400000,tcp,al low,686,620,66,4,2016/11/15 08:46:32,0,any,0,2816306064, 0x0,US,US,0,3,1,n/a,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:46:32 10.1.0.2 1,2016/ 11/15 08:46:32,001801015967, TRAFFIC,start,1,2016/11/15 0 8:46:32,209.67.78.56,50.232. 155.145,209.67.78.56,10.250. 0.10,inbound-web-browsing,,,

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0
8:46:32,15858,1,37151,80,371 51,80,0x400000,tcp,allow,703 ,629,74,4,2016/11/15 08:46:3
1,0,any,0,2816305976,0x0,US, US,0,3,1,n/a,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 6:31 10.1.0.2 1,2016/11/15 0 8:46:31,001801015967,TRAFFIC ,start,1,2016/11/15
08:46:31 ,205.173.105.205,50.232.155. 145,205.173.105.205,10.250.0 .10,inbound-
web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-
secureworks,2016/11/15 08 :46:31,38380,1,33247,80,3324 7,80,0x400000,tcp,allow,471,
405,66,4,2016/11/15 08:46:31 ,0,any,0,2816305969,0x0,US,U S,0,3,1,n/a,0,0,0,0,,ATL-PAN
-01,from-policy
Nov 15 08:46 :32 10.1.0.2 1,2016/11/15 08 :46:32,001801015967,TRAFFIC, start,1,2016/11/15
08:46:32, 64.85.77.2,50.232.155.145,64 .85.77.2,10.250.0.10,inbound -web-browsing,,,web-
browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15
08:46:32,2439 75,1,60691,80,60691,80,0x400 000,tcp,allow,684,610,74,4,2 016/11/15
08:46:32,0,any,0,2 816306017,0x0,US,US,0,3,1,n/ a,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:46:31 10.1.0 .2 1,2016/11/15 08:46:31,001 801015967,TRAFFIC,start,1,20
16/11/15 08:46:31,205.173.10 5.205,50.232.155.145,205.173 .105.205,10.250.0.10,inbound
-web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo
rks,2016/11/15 08:46:31,4002 6,1,65288,80,65288,80,0x4000 00,tcp,allow,663,597,66,4,20
16/11/15 08:46:31,0,any,0,28 16305946,0x0,US,US,0,3,1,n/a ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:46:31 10.1.0. 2 1,2016/11/15 08:46:31,0018 01015967,TRAFFIC,start,1,201
6/11/15 08:46:31,205.173.105 .205,50.232.155.145,205.173. 105.205,10.250.0.10,inbound-
web-browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-securewor
ks,2016/11/15 08:46:31,25288 ,1,63163,80,63163,80,0x40000 0,tcp,allow,566,500,66,4,201
6/11/15 08:46:31,0,any,0,281 6305938,0x0,US,US,0,3,1,n/a, 0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:46:31 10.1.0.2 1,2016/11/15 08:46:31,00180
1015967,TRAFFIC,start,1,2016 /11/15 08:46:31,205.173.105.
205,50.232.155.145,205.173.1 05.205,10.250.0.10,inbound-w eb-browsing,,,web-browsing,v
sys1,outside,dmz,ethernet1/4 ,ethernet1/2,dell-securework s,2016/11/15 08:46:31,33789,
1,32259,80,32259,80,0x400000 ,tcp,allow,678,612,66,4,2016 /11/15 08:46:31,0,any,0,2816
305950,0x0,US,US,0,3,1,n/a,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:46:31 10.1.0.2 1,2016/11/15 08:46:31,001801 015967,TRAFFIC,start,1,2016/
11/15 08:46:31,64.179.192.42 ,50.232.155.145,64.179.192.4 2,10.250.0.10,inbound-web-
br owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

6/11/15 08:46:31,43720,1,400 16,80,40016,80,0x400000,tcp, allow,1203,1137,66,4,2016/11 /15 08:46:22,9,any,0,2816305 963,0x0,US,US,0,3,1,n/a,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:31 10.1.0.2 1,2 016/11/15 08:46:31,001801015 967,TRAFFIC,end,1,2016/11/15 08:46:31,66.192.63.2,50.232 .155.145,66.192.63.2,10.250. 0.10,inbound-web-browsing,,, web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0 8:46:31,29192,1,12667,80,126 67,80,0x40001c,tcp,allow,786 02,18150,60452,71,2016/11/15 08:45:52,23,government,0,28 16305889,0x0,US,US,0,27,44,t cp-rst-from-client,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:46:30 10.1.0.2 1,2016/1 1/15 08:46:30,001801015967,T RAFFIC,end,1,2016/11/15 08:4 6:30,68.184.179.22,50.232.15 5.145,68.184.179.22,10.250.0 .10,inbound-web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15 08 :46:30,39510,1,59186,80,5918 6,80,0x40001c,tcp,allow,2394 ,809,1585,9,2016/11/15 08:44 :17,117,government,0,2816305 820,0x0,US,US,0,6,3,tcp-fin, 0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:46:30 10.1.0.2 1,2016/11/15 08:46:30,00180 1015967,TRAFFIC,end,1,2016/1 1/15 08:46:30,158.111.236.10 ,50.232.155.145,158.111.236. 10,10.250.0.10,inbound-web-b rowsing,,,web-browsing,vsys1 ,outside,dmz,ethernet1/4,eth ernet1/2,dell-secureworks,20 16/11/15 08:46:30,16146,1,23 484,80,23484,80,0x40001a,tcp ,allow,2278,757,1521,6,2016/ 11/15 08:46:14,0,government, 0,2816305781,0x0,US,US,0,4,2 ,tcp-rst-from-client,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:46:30 10.1.0.2 1,2016 /11/15 08:46:30,001801015967 ,TRAFFIC,start,1,2016/11/15 08:46:30,207.99.81.78,50.232 .155.145,207.99.81.78,10.250 .0.10,inbound-web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15 08:46:30,28540,1,2623,80,262 3,80,0x400000,tcp,allow,635, 573,62,4,2016/11/15 08:46:30 ,0,any,0,2816305845,0x0,US,U S,0,3,1,n/a,0,0,0,0,,ATL-PAN -01,from-policy
Nov 15 08:46 :30 10.1.0.2 1,2016/11/15 08 :46:30,001801015967,TRAFFIC, end,1,2016/11/15 08:46:30,68 .184.179.22,50.232.155.145,6 8.184.179.22,10.250.0.10,inb ound-web-browsing,,,incomple te,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure works,2016/11/15 08:46:30,35 455,1,59185,80,59185,80,0x40 001b,tcp,allow,312,186,126,5 ,2016/11/15 08:44:17,117,any ,0,2816305775,0x0,US,US,0,3, 2,tcp-rst-from-server,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:46:29 10.1.0.2 1,201 6/11/15 08:46:29,00180101596 7,TRAFFIC,start,1,2016/11/15 08:46:29,64.85.97.190,50.23 2.155.145,64.85.97.190,10.25 0.0.10,inbound-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15 08:46:29,12683,1,53666,80,5 3666,80,0x400000,tcp,allow,650,576,74,4,2016/11/15 08:46 :28,0,any,0,2816305667,0x0,U S,US,0,3,1,n/a,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08 :46:29 10.1.0.2 1,2016/11/15 08:46:29,001801015967,TRAFF IC,start,1,2016/11/15 08:46: 29,47.32.70.122,50.232.155.1 45,47.32.70.122,10.250.0.10, inbound-web-browsing,,,web-b rowsing,vsys1,outside,dmz,et hernet1/4,ethernet1/2,dell-s ecureworks,2016/11/15 08:46: 29,29061,1,54717,80,54717,80 ,0x400000,tcp,allow,1099,1033,66,4,2016/11/15 08:46:29,0 ,any,0,2816305739,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:2 9 10.1.0.2 1,2016/11/15 08:4 6:29,001801015967,TRAFFIC,st art,1,2016/11/15 08:46:29,47 .32.70.122,50.232.155.145,47 .32.70.122,10.250.0.10,inbou nd-web-browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure works,2016/11/15 08:46:29,40 902,1,54721,80,54721,80,0x40 0000,tcp,allow,480,414,66,4, 2016/11/15 08:46:29,0,any,0, 2816305747,0x0,US,US,0,3,1,n /a,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:29 10.1. 0.2 1,2016/11/15 08:46:29,00 1801015967,TRAFFIC,start,1,2016/11/15 08:46:29,47.32.70. 122,50.232.155.145,47.32.70. 122,10.250.0.10,inbound-web-browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2016/11/15 08:46:29,53754,1,5 4716,80,54716,80,0x400000,tc p,allow,1137,1071,66,4,2016/11/15 08:46:29,0,any,0,28163 05742,0x0,US,US,0,3,1,n/a,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:46:29 10.1.0.2 1 ,2016/11/15 08:46:29,0018010 15967,TRAFFIC,start,1,2016/11/15 08:46:29,47.32.70.122,5 0.232.155.145,47.32.70.122,1 0.250.0.10,inbound-web-browsing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/11/15 08:46:29,34111,1,54718, 80,54718,80,0x400000,tcp,all ow,1174,1108,66,4,2016/11/15 08:46:29,0,any,0,2816305745 ,0x0,US,US,0,3,1,n/a,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:46:29 10.1.0.2 1,2016 /11/15 08:46:29,001801015967 ,TRAFFIC,end,1,2016/11/15 08 :46:29,96.86.229.133,50.232. 155.145,96.86.229.133,10.250 .0.10,inbound-web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15 08:46:29,44591,1,19687,80,19 687,80,0x40001c,tcp,allow,66237,2773,63464,75,2016/11/15 08:46:10,3,government,0,281 6305713,0x0,US,US,0,30,45,tcp-fin,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:46:29 10 .1.0.2 1,2016/11/15 08:46:29 ,001801015967,TRAFFIC,end,1, 2016/11/15 08:46:29,64.85.97 .159,50.232.155.145,64.85.97 .159,10.250.0.10,inbound-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15 08:46:29,41723,1, 48970,80,48970,80,0x40001c,tcp,allow,39526,8205,31321,56 ,2016/11/15 08:46:12,1,government,0,2816305682,0x0,US,US ,0,31,25,tcp-rst-from-client ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:46:28 10.1.0. 2 1,2016/11/15 08:46:28,0018 01015967,TRAFFIC,start,1,2016/11/15 08:46:28,64.85.97.22 7,50.232.155.145,64.85.97.22 7,10.250.0.10,inbound-web-browsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,2016/11/15 08:46:28,52889,1,358 03,80,35803,80,0x400000,tcp, allow,684,610,74,4,2016/11/1 5 08:46:27,0,any,0,281630565 2,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:46:28 10.1.0.2 1,201 6/11/15 08:46:28,00180101596 7,TRAFFIC,end,1,2016/11/15 0 8:46:28,64.85.97.192,50.232. 155.145,64.85.97.192,10.250. 0.10,inbound-web-browsing,,,web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0 8:46:28,48096,1,60298,80,602 98,80,0x40001c,tcp,allow,190 76,5532,13544,44,2016/11/15 08:45:59,13,government,0,281 6305638,0x0,US,US,0,28,16,tc p-fin,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:46:28 10 .1.0.2 1,2016/11/15 08:46:28 ,001801015967,TRAFFIC,end,1, 2016/11/15 08:46:28,12.48.15 1.106,50.232.155.145,12.48.1 51.106,10.250.0.10,inbound-w eb-browsing,,,web-browsing,v sys1,outside,dmz,ethernet1/4 ,ethernet1/2,dell-securework s,2016/11/15 08:46:28,50004, 1,45632,80,45632,80,0x40001a ,tcp,allow,49441,9611,39830, 68,2016/11/15 08:46:03,9,gov ernment,0,2816305640,0x0,US, US,0,34,34,tcp-rst-from-client,0,0,0,0,,ATL-PAN-01,from- policy
Nov 15 08:46:26 10.1. 0.2 1,2016/11/15 08:46:26,00 1801015967,TRAFFIC,start,1,2016/11/15 08:46:26,104.182.2 06.4,50.232.155.145,104.182. 206.4,10.250.0.10,inbound-we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-secureworks ,2016/11/15 08:46:26,43140,1 ,63265,80,63265,80,0x400000, tcp,allow,6505,6439,66,7,201 6/11/15 08:46:24,2,any,0,281 6305555,0x0,US,US,0,6,1,n/a, 0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:46:26 10.1.0.2 1,2016/11/15 08:46:26,00180 1015967,TRAFFIC,end,1,2016/11/15 08:46:26,207.99.81.78,5 0.232.155.145,207.99.81.78,1 0.250.0.10,inbound-web-browsing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/11/15 08:46:26,24476,1,2621,8 0,2621,80,0x40001a,tcp,allow ,2341,766,1575,8,2016/11/15 08:46:10,0,government,0,2816 305533,0x0,US,US,0,5,3,tcp-r st-from-client,0,0,0,0,,ATL-PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08 :46:26 10.1.0.2 1,2016/11/15 08:46:26,001801015967,TRAFF IC,end,1,2016/11/15 08:46:26 ,67.198.62.57,50.232.155.145 ,67.198.62.57,10.250.0.10,in bound-web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec ureworks,2016/11/15 08:46:26 ,38502,1,61295,80,61295,80,0 x40001c,tcp,allow,57327,9660 ,47667,70,2016/11/15 08:45:5 8,12,government,0,2816305536 ,0x0,US,US,0,32,38,tcp-rst-f rom-client,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46: 24 10.1.0.2 1,2016/11/15 08: 46:24,001801015967,TRAFFIC,s tart,1,2016/11/15 08:46:24,7 4.174.56.6,50.232.155.145,74 .174.56.6,10.250.0.10,inboun d-web-browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew orks,2016/11/15 08:46:24,330 17,1,32281,80,32281,80,0x400 000,tcp,allow,1270,1204,66,4 ,2016/11/15 08:46:24,0,any,0 ,2816305425,0x0,US,US,0,3,1, n/a,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:46:24 10.1 .0.2 1,2016/11/15 08:46:24,0 01801015967,TRAFFIC,start,1, 2016/11/15 08:46:24,74.174.5 6.6,50.232.155.145,74.174.56 .6,10.250.0.10,inbound-web-b rowsing,,,web-browsing,vsys1 ,outside,dmz,ethernet1/4,eth ernet1/2,dell-secureworks,20 16/11/15 08:46:24,54281,1,11 992,80,11992,80,0x400000,tcp ,allow,1173,1107,66,4,2016/1 1/15 08:46:24,0,any,0,281630 5427,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:25 10.1.0.2 1, 2016/11/15 08:46:25,00180101 5967,TRAFFIC,end,1,2016/11/1 5 08:46:25,12.206.16.210,50. 232.155.145,12.206.16.210,10 .250.0.10,inbound-web-browsi ng,,,incomplete,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5 08:46:25,43836,1,52450,80, 52450,80,0x40001b,tcp,allow, 312,186,126,5,2016/11/15 08: 46:03,6,any,0,2816305452,0x0 ,US,US,0,3,2,tcp-rst-from-se rver,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:46:25 10. 1.0.2 1,2016/11/15 08:46:25, 001801015967,TRAFFIC,end,1,2 016/11/15 08:46:25,12.206.16 .210,50.232.155.145,12.206.1 6.210,10.250.0.10,inbound-we b-browsing,,,incomplete,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2 016/11/15 08:46:25,129757,1, 52448,80,52448,80,0x40001b,t cp,allow,312,186,126,5,2016/ 11/15 08:46:03,6,any,0,28163 05462,0x0,US,US,0,3,2,tcp-rs t-from-server,0,0,0,0,,ATL-P AN-01,from-policy
Nov 15 08: 46:25 10.1.0.2 1,2016/11/15 08:46:25,001801015967,TRAFFI C,end,1,2016/11/15 08:46:25, 12.206.16.210,50.232.155.145 ,12.206.16.210,10.250.0.10,i nbound-web-browsing,,,incomp lete,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu reworks,2016/11/15 08:46:25, 36909,1,52449,80,52449,80,0x

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

40001b,tcp,allow,312,186,126 ,5,2016/11/15 08:46:03,6,any ,0,2816305472,0x0,US,US,0,3,
2,tcp-rst-from-server,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:46:24 10.1.0.2 1,201 6/11/15 08:46:24,00180101596 7,TRAFFIC,start,1,2016/11/15
08:46:24,74.174.56.6,50.232 .155.145,74.174.56.6,10.250. 0.10,inbound-web-browsing,,,
web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15
0 8:46:24,25943,1,63694,80,636 94,80,0x400000,tcp,allow,124 3,1177,66,4,2016/11/15
08:46 :23,1,any,0,2816305424,0x0,U S,US,0,3,1,n/a,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :46:24 10.1.0.2 1,2016/11/15 08:46:24,001801015967,TRAFF IC,start,1,2016/11/15
08:46: 24,74.174.56.6,50.232.155.14 5,74.174.56.6,10.250.0.10,in bound-web-browsing,,,web-
bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec ureworks,2016/11/15
08:46:24 ,42179,1,63726,80,63726,80,0 x400000,tcp,allow,1173,1107, 66,4,2016/11/15
08:46:24,0,a ny,0,2816305426,0x0,US,US,0, 3,1,n/a,0,0,0,0,,ATL-PAN-01, from-policy
Nov 15 08:46:24 10.1.0.2 1,2016/11/15 08:46: 24,001801015967,TRAFFIC,star t,1,2016/11/15
08:46:24,74.1 74.56.6,50.232.155.145,74.17 4.56.6,10.250.0.10,inbound-w eb-browsing,,,web-
browsing,v sys1,outside,dmz,ethernet1/4 ,ethernet1/2,dell-securework s,2016/11/15
08:46:24,22988, 1,29843,80,29843,80,0x400000 ,tcp,allow,1172,1106,66,4,20 16/11/15
08:46:23,0,any,0,28 16305403,0x0,US,US,0,3,1,n/a ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:46:23 10.1.0. 2 1,2016/11/15 08:46:23,0018 01015967,TRAFFIC,end,1,2016/
11/15 08:46:23,152.133.7.129 ,50.232.155.145,152.133.7.12 9,10.250.0.10,inbound-
web-br owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-
secureworks,201 6/11/15 08:46:23,31653,1,616 85,80,61685,80,0x40001a,tcp,
allow,4866,2747,2119,19,2016 /11/15 08:45:47,20,governmen
t,0,2816305297,0x0,US,US,0,7 ,12,tcp-rst-from-client,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:23 10.1.0.2 1,2 016/11/15 08:46:23,001801015 967,TRAFFIC,end,1,2016/11/15
08:46:23,64.85.77.2,50.232. 155.145,64.85.77.2,10.250.0. 10,inbound-web-browsing,,,we
b-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08:
46:23,53071,1,60410,80,60410 ,80,0x40001c,tcp,allow,39096 ,7840,31256,49,2016/11/15
08 :45:58,9,government,0,281630 5277,0x0,US,US,0,25,24,tcp-f in,0,0,0,0,,ATL-PAN-01,from-
policy
Nov 15 08:46:23 10.1. 0.2 1,2016/11/15 08:46:23,00 1801015967,TRAFFIC,end,1,201
6/11/15 08:46:23,208.87.238. 180,50.232.155.145,208.87.23 8.180,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-
secureworks ,2016/11/15 08:46:23,13399,1 ,35678,80,35678,80,0x40001c,

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

tcp,allow,15592,2718,12874,2 9,2016/11/15 08:45:46,21,gov ernment,0,2816305289,0x0,US,
US,0,16,13,tcp-fin,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:46:22 10.1.0.2 1,2016/1 1/15 08:46:22,001801015967,T RAFFIC,start,1,2016/11/15
08 :46:22,152.133.7.129,50.232. 155.145,152.133.7.129,10.250 .0.10,inbound-
web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-
secureworks,2016/11/15 08:46:22,42821,1,24166,80,24 166,80,0x400000,tcp,allow,16
06,1540,66,4,2016/11/15 08:4 6:22,0,any,0,2816305263,0x0, US,US,0,3,1,n/a,0,0,0,0,,ATL -
PAN-01,from-policy
Nov 15 0 8:46:23 10.1.0.2 1,2016/11/1 5 08:46:23,001801015967,TRAF FIC,start,1,2016/11/15
08:46 :23,64.85.77.13,50.232.155.1 45,64.85.77.13,10.250.0.10,i nbound-web-browsing,,,web-
br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15 08:46:2
3,37215,1,34808,80,34808,80, 0x400000,tcp,allow,684,610,7 4,4,2016/11/15 08:46:22,0,an
y,0,2816305314,0x0,US,US,0,3 ,1,n/a,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:46:23 1 0.1.0.2 1,2016/11/15 08:46:2 3,001801015967,TRAFFIC,end,1 ,2016/11/15
08:46:23,64.85.9 7.241,50.232.155.145,64.85.9 7.241,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-
secureworks ,2016/11/15 08:46:23,42014,1 ,56713,80,56713,80,0x40001c,
tcp,allow,6848,2753,4095,21, 2016/11/15 08:46:05,2,govern ment,0,2816305294,0x0,US,US,
0,14,7,tcp-rst-from-client,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:46:22 10.1.0.2 1,2016/11/15 08:46:22,001801 015967,TRAFFIC,drop,1,2016/1
1/15 08:46:22,14.109.151.150 ,50.232.155.145,0.0.0.0,0.0. 0.0,deny-remaining,,,not-
app licable,vsys1,outside,dmz,et hernet1/4,,dell-secureworks, 2016/11/15
08:46:22,0,1,1433 4,23,0,0,0x0,tcp,deny,60,60, 0,1,2016/11/15 08:46:22,0,an
y,0,2816305247,0x0,CN,US,0,1 ,0,policy-deny,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :46:22 10.1.0.2 1,2016/11/15 08:46:22,001801015967,TRAFF IC,start,1,2016/11/15
08:46: 22,66.192.63.2,50.232.155.14 5,66.192.63.2,10.250.0.10,in bound-web-browsing,,,web-
bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec ureworks,2016/11/15
08:46:22 ,34026,1,64531,80,64531,80,0 x400000,tcp,allow,1523,1449, 74,4,2016/11/15
08:46:22,0,a ny,0,2816305246,0x0,US,US,0, 3,1,n/a,0,0,0,0,,ATL-PAN-01, from-policy
Nov 15 08:46:22 10.1.0.2 1,2016/11/15 08:46: 22,001801015967,TRAFFIC,star
t,1,2016/11/15 08:46:22,207. 99.81.78,50.232.155.145,207.
99.81.78,10.250.0.10,inbound -web-browsing,,,web-
browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

08:46:22,4624 8,1,2622,80,2622,80,0x400000 ,tcp,allow,691,629,62,4,2016 /11/15
08:46:21,1,any,0,2816 305238,0x0,US,US,0,3,1,n/a,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:46:22 10.1.0.2 1,2016/11/15 08:46:22,001801 015967,TRAFFIC,start,1,2016/
11/15 08:46:22,152.133.7.129 ,50.232.155.145,152.133.7.12 9,10.250.0.10,inbound-web-
br owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201
6/11/15 08:46:22,18634,1,450 77,80,45077,80,0x400000,tcp, allow,1606,1540,66,4,2016/11 /15
08:46:22,0,any,0,2816305 248,0x0,US,US,0,3,1,n/a,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:21 10.1.0.2 1,2 016/11/15 08:46:21,001801015 967,TRAFFIC,start,1,2016/11/
15 08:46:21,64.85.77.4,50.23 2.155.145,64.85.77.4,10.250. 0.10,inbound-web-browsing,,,
web-browsing,vsys1,outside,d mz,ethernet1/4,ethernet1/2,d ell-secureworks,2016/11/15 0
8:46:21,41812,1,32781,80,327 81,80,0x400000,tcp,allow,612 ,538,74,4,2016/11/15 08:46:2
0,1,any,0,2816305180,0x0,US, US,0,3,1,n/a,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 6:21 10.1.0.2 1,2016/11/15 0 8:46:21,001801015967,TRAFFIC ,start,1,2016/11/15
08:46:21 ,174.218.130.192,50.232.155. 145,174.218.130.192,10.250.0 .10,inbound-
web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-
secureworks,2016/11/15 08 :46:21,46644,1,7181,80,7181, 80,0x400000,tcp,allow,698,62
4,74,4,2016/11/15 08:46:21,0 ,any,0,2816305181,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-0
1,from-policy
Nov 15 08:46:2 1 10.1.0.2 1,2016/11/15 08:4 6:21,001801015967,TRAFFIC,st art,1,2016/11/15
08:46:21,15 2.133.7.129,50.232.155.145,1 52.133.7.129,10.250.0.10,inb ound-
web-browsing,,,web-brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu
reworks,2016/11/15 08:46:21, 35709,1,61699,80,61699,80,0x 400000,tcp,allow,1606,1540,6
6,4,2016/11/15 08:45:51,30,a ny,0,2816305184,0x0,US,US,0, 3,1,n/a,0,0,0,0,,ATL-PAN-01,
from-policy
Nov 15 08:46:20 10.1.0.2 1,2016/11/15 08:46: 20,001801015967,TRAFFIC,star t,1,2016/11/15
08:46:20,70.1 33.222.130,50.232.155.145,70 .133.222.130,10.250.0.10,inb ound-
web-browsing,,,web-brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu
reworks,2016/11/15 08:46:20, 45867,1,61086,80,61086,80,0x 400000,tcp,allow,528,454,74,
4,2016/11/15 08:46:20,0,any, 0,2816305135,0x0,US,US,0,3,1 ,n/a,0,0,0,0,,ATL-PAN-01,fro m-
policy
Nov 15 08:46:20 10. 1.0.2 1,2016/11/15 08:46:20, 001801015967,TRAFFIC,start,1 ,2016/11/15
08:46:20,70.133. 222.130,50.232.155.145,70.13 3.222.130,10.250.0.10,inboun d-web-
browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew
orks,2016/11/15 08:46:20,470 67,1,61085,80,61085,80,0x400 000,tcp,allow,642,568,74,4,2

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

016/11/15 08:46:20,0,any,0,2 816305133,0x0,US,US,0,3,1,n/ a,0,0,0,0,,ATL-PAN-01,from-p
olicy
Nov 15 08:46:21 10.1.0 .2 1,2016/11/15 08:46:21,001
801015967,TRAFFIC,start,1,20 16/11/15 08:46:21,174.218.13
0.192,50.232.155.145,174.218 .130.192,10.250.0.10,inbound -web-browsing,,,web-
browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15
08:46:21,5363 3,1,7195,80,7195,80,0x400000 ,tcp,allow,724,650,74,4,2016 /11/15
08:46:20,1,any,0,2816 305179,0x0,US,US,0,3,1,n/a,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:46:21 10.1.0.2 1,2016/11/15 08:46:21,001801 015967,TRAFFIC,start,1,2016/
11/15 08:46:21,174.218.130.1 92,50.232.155.145,174.218.13 0.192,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-
secureworks ,2016/11/15 08:46:21,47675,1 ,7198,80,7198,80,0x400000,tc
p,allow,670,596,74,4,2016/11 /15 08:46:20,0,any,0,2816305 176,0x0,US,US,0,3,1,n/a,0,0,
0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:20 10.1.0.2 1,2 016/11/15 08:46:20,001801015 967,TRAFFIC,start,1,2016/11/ 15
08:46:20,64.85.77.13,50.2 32.155.145,64.85.77.13,10.25 0.0.10,inbound-web-browsing, ,,web-
browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15
08:46:20,44150,1,44945,80,4 4945,80,0x400000,tcp,allow,6 03,529,74,4,2016/11/15
08:46 :20,0,any,0,2816305122,0x0,U S,US,0,3,1,n/a,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :46:20 10.1.0.2 1,2016/11/15 08:46:20,001801015967,TRAFF IC,start,1,2016/11/15
08:46: 20,66.110.201.211,50.232.155 .145,66.110.201.211,10.250.0 .10,inbound-
web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de
ll-secureworks,2016/11/15 08 :46:20,46896,1,62804,80,6280
4,80,0x400000,tcp,allow,1707 ,1633,74,4,2016/11/15 08:46:
19,1,any,0,2816305112,0x0,US ,US,0,3,1,n/a,0,0,0,0,,ATL-P AN-01,from-policy
Nov 15 08: 46:20 10.1.0.2 1,2016/11/15 08:46:20,001801015967,TRAFFI C,start,1,2016/11/15
08:46:2 0,64.85.77.10,50.232.155.145 ,64.85.77.10,10.250.0.10,inb ound-web-browsing,,,web-
brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu reworks,2016/11/15 08:46:20,
39032,1,41856,80,41856,80,0x 400000,tcp,allow,600,526,74, 4,2016/11/15 08:46:20,0,any,
0,2816305115,0x0,US,US,0,3,1 ,n/a,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:46:20 10. 1.0.2 1,2016/11/15 08:46:20, 001801015967,TRAFFIC,end,1,2
016/11/15 08:46:20,12.206.16 .210,50.232.155.145,12.206.1 6.210,10.250.0.10,inbound-
we b-browsing,,,incomplete,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2
016/11/15 08:46:20,38408,1,5 2447,80,52447,80,0x40001b,tc p,allow,312,186,126,5,2016/1

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

1/15 08:45:59,5,any,0,281630 5109,0x0,US,US,0,3,2,tcp-rst -from-server,0,0,0,0,,ATL-PA
N-01,from-policy
Nov 15 08:4 6:20 10.1.0.2 1,2016/11/15 0 8:46:20,001801015967,TRAFFIC ,end,1,2016/11/15
08:46:20,1 04.129.204.75,50.232.155.145 ,104.129.204.75,10.250.0.10, inbound-
web-browsing,,,web-b rowsing,vsys1,outside,dmz,et hernet1/4,ethernet1/2,dell-s
ecureworks,2016/11/15 08:46: 20,36279,1,40444,80,40444,80 ,0x40001a,tcp,allow,74266,14
006,60260,88,2016/11/15 08:4 5:54,10,government,0,2816305 107,0x0,US,US,0,41,47,tcp-rs t-
from-client,0,0,0,0,,ATL-P AN-01,from-policy
Nov 15 08: 46:19 10.1.0.2 1,2016/11/15 08:46:19,001801015967,TRAFFI C,end,1,2016/11/15
08:46:19, 76.125.21.93,50.232.155.145, 76.125.21.93,10.250.0.10,inb ound-web-
browsing,,,web-brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu
reworks,2016/11/15 08:46:19, 36480,1,52845,80,52845,80,0x 40001c,tcp,allow,19032,3792,
15240,41,2016/11/15 08:45:13 ,50,government,0,2816304943, 0x0,US,US,0,23,18,tcp-rst-fr
om-server,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:46:1 9 10.1.0.2 1,2016/11/15 08:4 6:19,001801015967,TRAFFIC,en d,1,2016/11/15
08:46:19,64.8 5.77.4,50.232.155.145,64.85. 77.4,10.250.0.10,inbound-web -browsing,,,web-
browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15
08:46:19,38423,1, 37036,80,37036,80,0x40001c,t cp,allow,96173,12066,84107,1
16,2016/11/15 08:45:13,50,go vernment,0,2816304937,0x0,US ,US,0,52,64,tcp-rst-from-cli
ent,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:46:17 10.1 .0.2 1,2016/11/15 08:46:17,0 01801015967,TRAFFIC,start,1, 2016/11/15
08:46:17,74.174.5 6.6,50.232.155.145,74.174.56 .6,10.250.0.10,inbound-web-b rowsing,,,web-
browsing,vsys1 ,outside,dmz,ethernet1/4,eth ernet1/2,dell-secureworks,20 16/11/15
08:46:17,46498,1,63 722,80,63722,80,0x400000,tcp ,allow,1119,1053,66,4,2016/1 1/15
08:46:17,0,any,0,281630 4639,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:17 10.1.0.2 1, 2016/11/15 08:46:17,00180101 5967,TRAFFIC,start,1,2016/11 /15
08:46:17,74.174.56.6,50. 232.155.145,74.174.56.6,10.2 50.0.10,inbound-web-browsing ,,,web-
browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5
08:46:17,182728,1,17230,80 ,17230,80,0x400000,tcp,allow ,1236,1170,66,4,2016/11/15 0
8:46:17,0,any,0,2816304641,0 x0,US,US,0,3,1,n/a,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:46:17 10.1.0.2 1,2016/1 1/15 08:46:17,001801015967,T RAFFIC,start,1,2016/11/15
08 :46:17,209.67.78.58,50.232.1 55.145,209.67.78.58,10.250.0 .10,inbound-web-browsing,,,w
eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

08 :46:17,42022,1,39192,80,3919 2,80,0x400000,tcp,allow,684, 610,74,4,2016/11/15 08:46:17 ,0,any,0,2816304649,0x0,US,U S,0,3,1,n/a,0,0,0,0,,ATL-PAN -01,from-policy
Nov 15 08:46 :17 10.1.0.2 1,2016/11/15 08 :46:17,001801015967,TRAFFIC, start,1,2016/11/15 08:46:17, 74.174.56.6,50.232.155.145,7 4.174.56.6,10.250.0.10,inbou nd-web-browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure works,2016/11/15 08:46:17,41 351,1,48456,80,48456,80,0x40 0000,tcp,allow,1139,1073,66, 4,2016/11/15 08:46:17,0,any, 0,2816304642,0x0,US,US,0,3,1 ,n/a,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:46:17 10. 1.0.2 1,2016/11/15 08:46:17, 001801015967,TRAFFIC,start,1 ,2016/11/15 08:46:17,74.174. 56.6,50.232.155.145,74.174.5 6.6,10.250.0.10,inbound-web- browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2 016/11/15 08:46:17,45125,1,1 1383,80,11383,80,0x400000,tc p,allow,1209,1143,66,4,2016/ 11/15 08:46:17,0,any,0,28163 04640,0x0,US,US,0,3,1,n/a,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:46:17 10.1.0.2 1 ,2016/11/15 08:46:17,0018010 15967,TRAFFIC,end,1,2016/11/ 15 08:46:17,209.67.78.55,50. 232.155.145,209.67.78.55,10. 250.0.10,inbound-web-browsin g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15 08:46:17,249448,1,38727,8 0,38727,80,0x40001c,tcp,allo w,62517,6989,55528,97,2016/1 1/15 08:45:50,11,government, 0,2816304616,0x0,US,US,0,53, 44,tcp-rst-from-client,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:46:17 10.1.0.2 1,20 16/11/15 08:46:17,0018010159 67,TRAFFIC,start,1,2016/11/1 5 08:46:17,64.85.77.12,50.23 2.155.145,64.85.77.12,10.250 .0.10,inbound-web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15 08:46:17,45270,1,52197,80,52 197,80,0x400000,tcp,allow,68 9,615,74,4,2016/11/15 08:46: 16,0,any,0,2816304635,0x0,US ,US,0,3,1,n/a,0,0,0,0,,ATL-P AN-01,from-policy
Nov 15 08: 46:16 10.1.0.2 1,2016/11/15 08:46:16,001801015967,TRAFFI C,start,1,2016/11/15 08:46:1 6,64.85.97.180,50.232.155.14 5,64.85.97.180,10.250.0.10,i nbound-web-browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15 08:46:1 6,26313,1,51694,80,51694,80, 0x400000,tcp,allow,618,544,7 4,4,2016/11/15 08:46:16,0,an y,0,2816304602,0x0,US,US,0,3 ,1,n/a,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:46:16 1 0.1.0.2 1,2016/11/15 08:46:1 6,001801015967,TRAFFIC,end,1 ,2016/11/15 08:46:16,64.85.9 7.171,50.232.155.145,64.85.9 7.171,10.250.0.10,inbound-we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-secureworks ,2016/11/15 08:46:16,38529,1 ,50050,80,50050,80,0x40001c,

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

tcp,allow,2341,730,1611,9,20 16/11/15 08:46:00,0,governme nt,0,2816304564,0x0,US,US,0,
6,3,tcp-rst-from-client,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:16 10.1.0.2 1,2 016/11/15 08:46:16,001801015 967,TRAFFIC,end,1,2016/11/15
08:46:16,64.85.77.14,50.232 .155.145,64.85.77.14,10.250. 0.10,inbound-web-browsing,,,
incomplete,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15
08: 46:16,33098,1,49037,80,49037 ,80,0x40001b,tcp,allow,340,2 06,134,5,2016/11/15
08:46:00 ,0,any,0,2816304567,0x0,US,U S,0,3,2,tcp-rst-from-server, 0,0,0,0,,ATL-PAN-01,from-
pol icy
Nov 15 08:46:15 10.1.0.2 1,2016/11/15 08:46:15,00180 1015967,TRAFFIC,start,1,2016 /11/15
08:46:15,64.85.97.207 ,50.232.155.145,64.85.97.207 ,10.250.0.10,inbound-
web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-
secureworks,2016 /11/15 08:46:15,46220,1,5393 8,80,53938,80,0x400000,tcp,a
llow,603,529,74,4,2016/11/15 08:46:15,0,any,0,2816304536 ,0x0,US,US,0,3,1,n/
a,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:46:16 10.1.0.2 1,2016 /11/15 08:46:16,001801015967 ,TRAFFIC,end,1,2016/11/15
08 :46:16,209.67.78.54,50.232.1 55.145,209.67.78.54,10.250.0 .10,inbound-
web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-
secureworks,2016/11/15 08 :46:16,35380,1,55666,80,5566 6,80,0x40001c,tcp,allow,1393
20,21574,117746,210,2016/11/ 15 08:45:25,35,government,0, 2816304553,0x0,US,US,0,115,9
5,tcp-fin,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:46:1 5 10.1.0.2 1,2016/11/15 08:4 6:15,001801015967,TRAFFIC,en d,1,2016/11/15
08:46:15,64.8 5.77.8,50.232.155.145,64.85. 77.8,10.250.0.10,inbound-web -browsing,,,web-
browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15
08:46:15,49108,1, 34626,80,34626,80,0x40001c,t cp,allow,19040,1715,17325,30 ,2016/11/15
08:45:46,13,gove rnment,0,2816304463,0x0,US,U S,0,14,16,tcp-fin,0,0,0,0,,A TL-PAN-01,from-
policy
Nov 15 08:46:15 10.1.0.2 1,2016/11 /15 08:46:15,001801015967,TR AFFIC,start,1,2016/11/15
08: 46:15,158.111.236.10,50.232. 155.145,158.111.236.10,10.25 0.0.10,inbound-
web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-
secureworks,2016/11/15 08:46:15,16146,1,23484,80,2 3484,80,0x400000,tcp,allow,7
59,697,62,4,2016/11/15 08:46 :14,0,any,0,2816304466,0x0,U S,US,0,3,1,n/a,0,0,0,0,,ATL-
PAN-01,from-policy
Nov 15 08 :46:15 10.1.0.2 1,2016/11/15 08:46:15,001801015967,TRAFF IC,start,1,2016/11/15
08:46: 15,158.111.236.10,50.232.155 .145,158.111.236.10,10.250.0 .10,inbound-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15 08 :46:15,51862,1,38665,80,3866 5,80,0x400000,tcp,allow,744, 682,62,4,2016/11/15 08:46:14 ,0,any,0,2816304435,0x0,US,U S,0,3,1,n/a,0,0,0,0,,ATL-PAN -01,from-policy
Nov 15 08:46 :14 10.1.0.2 1,2016/11/15 08 :46:14,001801015967,TRAFFIC, start,1,2016/11/15 08:46:14, 64.85.77.8,50.232.155.145,64 .85.77.8,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:46:14,3706 9,1,37866,80,37866,80,0x4000 00,tcp,allow,650,576,74,4,20 16/11/15 08:46:14,0,any,0,28 16304408,0x0,US,US,0,3,1,n/a ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:46:14 10.1.0. 2 1,2016/11/15 08:46:14,0018 01015967,TRAFFIC,start,1,201 6/11/15 08:46:14,158.111.236 .10,50.232.155.145,158.111.2 36.10,10.250.0.10,inbound-we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-secureworks ,2016/11/15 08:46:14,262107, 1,40201,80,40201,80,0x400000 ,tcp,allow,656,594,62,4,2016 /11/15 08:46:14,0,any,0,2816 304422,0x0,US,US,0,3,1,n/a,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:46:15 10.1.0.2 1,2016/11/15 08:46:15,001801 015967,TRAFFIC,start,1,2016/ 11/15 08:46:15,12.48.151.106 ,50.232.155.145,12.48.151.10 6,10.250.0.10,inbound-web-br owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201 6/11/15 08:46:15,26931,1,261 19,80,26119,80,0x400000,tcp, allow,695,629,66,4,2016/11/1 5 08:46:14,0,any,0,281630449 8,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:46:14 10.1.0.2 1,201 6/11/15 08:46:14,00180101596 7,TRAFFIC,start,1,2016/11/15 08:46:14,12.48.151.106,50.2 32.155.145,12.48.151.106,10. 250.0.10,inbound-web-browsin g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15 08:46:14,58830,1,64516,80 ,64516,80,0x400000,tcp,allow ,694,628,66,4,2016/11/15 08: 46:14,0,any,0,2816304425,0x0 ,US,US,0,3,1,n/a,0,0,0,0,,AT L-PAN-01,from-policy
Nov 15 08:46:15 10.1.0.2 1,2016/11/ 15 08:46:15,001801015967,TRA FFIC,start,1,2016/11/15 08:4 6:15,12.48.151.106,50.232.15 5.145,12.48.151.106,10.250.0 .10,inbound-web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15 08 :46:15,50174,1,1975,80,1975, 80,0x400000,tcp,allow,695,62 9,66,4,2016/11/15 08:46:14,1 ,any,0,2816304499,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:46:1 4 10.1.0.2 1,2016/11/15 08:4 6:14,001801015967,TRAFFIC,en d,1,2016/11/15 08:46:14,64.8 5.97.172,50.232.155.145,64.8 5.97.172,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

rks,2016/11/15 08:46:14,5704 8,1,37948,80,37948,80,0x4000 1c,tcp,allow,45735,10722,350
13,72,2016/11/15 08:45:52,6, government,0,2816304389,0x0, US,US,0,41,31,tcp-rst-from-c
lient,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:46:14 10 .1.0.2 1,2016/11/15 08:46:14 ,001801015967,TRAFFIC,end,1,
2016/11/15 08:46:14,207.99.8 1.78,50.232.155.145,207.99.8 1.78,10.250.0.10,inbound-web
-browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks,
2016/11/15 08:46:14,46703,1, 2618,80,2618,80,0x40001a,tcp ,allow,30539,3470,27069,40,2
016/11/15 08:45:28,30,govern ment,0,2816304370,0x0,US,US, 0,15,25,tcp-rst-from-client,
0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:46:14 10.1.0.2 1,2016/11/15 08:46:14,00180 1015967,TRAFFIC,end,1,2016/1
1/15 08:46:14,66.192.63.2,50 .232.155.145,66.192.63.2,10. 250.0.10,inbound-web-browsin
g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15
08:46:14,43786,1,31405,80 ,31405,80,0x40001c,tcp,allow ,75861,17000,58861,69,2016/1 1/15
08:44:51,67,government, 0,2816304367,0x0,US,US,0,26, 43,tcp-fin,0,0,0,0,,ATL-PAN- 01,from-
policy
Nov 15 08:46: 13 10.1.0.2 1,2016/11/15 08: 46:13,001801015967,TRAFFIC,s
tart,1,2016/11/15 08:46:13,1 08.226.66.78,50.232.155.145, 108.226.66.78,10.250.0.10,in
bound-web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-
sec ureworks,2016/11/15 08:46:13 ,56375,1,56709,80,56709,80,0
x400000,tcp,allow,724,658,66 ,4,2016/11/15 08:46:13,0,any ,0,2816304350,0x0,US,US,0,3,
1,n/a,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:46:13 10 .1.0.2 1,2016/11/15 08:46:13 ,001801015967,TRAFFIC,start, 1,2016/11/15
08:46:13,108.22 6.66.78,50.232.155.145,108.2 26.66.78,10.250.0.10,inbound -web-
browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo
rks,2016/11/15 08:46:13,3426 3,1,56707,80,56707,80,0x4000 00,tcp,allow,682,616,66,4,20
16/11/15 08:46:13,0,any,0,28 16304334,0x0,US,US,0,3,1,n/a ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:46:12 10.1.0. 2 1,2016/11/15 08:46:12,0018 01015967,TRAFFIC,start,1,201
6/11/15 08:46:12,64.85.77.4, 50.232.155.145,64.85.77.4,10 .250.0.10,inbound-web-browsi
ng,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15
08:46:12,55410,1,36032,8 0,36032,80,0x400000,tcp,allo w,689,615,74,4,2016/11/15
08 :46:11,0,any,0,2816304263,0x 0,US,US,0,3,1,n/a,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:46:12 10.1.0.2 1,2016/11 /15 08:46:12,001801015967,TR AFFIC,start,1,2016/11/15
08: 46:12,64.85.97.159,50.232.15 5.145,64.85.97.159,10.250.0. 10,inbound-web-browsing,,,we
b-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08:

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

46:12,41723,1,48970,80,48970 ,80,0x400000,tcp,allow,684,6 10,74,4,2016/11/15 08:46:12,
0,any,0,2816304282,0x0,US,US ,0,3,1,n/a,0,0,0,0,,ATL-PAN- 01,from-policy
Nov 15 08:46: 13 10.1.0.2 1,2016/11/15 08: 46:13,001801015967,TRAFFIC,e nd,1,2016/11/15
08:46:13,64. 85.77.13,50.232.155.145,64.8 5.77.13,10.250.0.10,inbound- web-browsing,,,web-
browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-securewor ks,2016/11/15
08:46:13,40049 ,1,47468,80,47468,80,0x40001 c,tcp,allow,32555,2640,29915 ,50,2016/11/15
08:45:32,25,g overnment,0,2816304301,0x0,U S,US,0,24,26,tcp-rst-from-cl ient,0,0,0,0,,ATL-
PAN-01,fro m-policy
Nov 15 08:46:11 10. 1.0.2 1,2016/11/15 08:46:11, 001801015967,TRAFFIC,start,1 ,2016/11/15
08:46:11,64.85.7 7.5,50.232.155.145,64.85.77. 5,10.250.0.10,inbound-web-br owsing,,,web-
browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201 6/11/15
08:46:11,43358,1,455 74,80,45574,80,0x400000,tcp, allow,612,538,74,4,2016/11/1 5
08:46:11,0,any,0,281630418 7,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:46:11 10.1.0.2 1,201 6/11/15 08:46:11,00180101596 7,TRAFFIC,start,1,2016/11/15
08:46:11,96.86.229.133,50.2 32.155.145,96.86.229.133,10. 250.0.10,inbound-web-browsin
g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/
15 08:46:11,30555,1,63258,80 ,63258,80,0x400000,tcp,allow ,568,494,74,4,2016/11/15 08:
46:11,0,any,0,2816304196,0x0 ,US,US,0,3,1,n/a,0,0,0,0,,AT L-PAN-01,from-policy
Nov 15 08:46:11 10.1.0.2 1,2016/11/ 15 08:46:11,001801015967,TRA FFIC,end,1,2016/11/15
08:46: 11,64.85.97.218,50.232.155.1 45,64.85.97.218,10.250.0.10, inbound-
web-browsing,,,web-b rowsing,vsys1,outside,dmz,et hernet1/4,ethernet1/2,dell-s
ecureworks,2016/11/15 08:46: 11,35303,1,51950,80,51950,80 ,0x40001c,tcp,allow,21568,37
85,17783,36,2016/11/15 08:45 :24,31,government,0,28163041 61,0x0,US,US,0,21,15,tcp-rst -
from-client,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 6:10 10.1.0.2 1,2016/11/15 0 8:46:10,001801015967,TRAFFIC ,start,1,2016/11/15
08:46:10 ,207.99.81.78,50.232.155.145 ,207.99.81.78,10.250.0.10,in bound-
web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-
sec ureworks,2016/11/15 08:46:10 ,24476,1,2621,80,2621,80,0x4
00000,tcp,allow,708,646,62,4 ,2016/11/15 08:46:10,0,any,0 ,2816304098,0x0,US,US,0,3,1, n/
a,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:46:10 10.1 .0.2 1,2016/11/15 08:46:10,0 01801015967,TRAFFIC,start,1,
2016/11/15 08:46:10,96.86.22 9.133,50.232.155.145,96.86.2
29.133,10.250.0.10,inbound-w eb-browsing,,,web-browsing,v
sys1,outside,dmz,ethernet1/4 ,ethernet1/2,dell-securework s,2016/11/15 08:46:10,44591,

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

1,19687,80,19687,80,0x400000 ,tcp,allow,633,559,74,4,2016 /11/15 08:46:10,0,any,0,2816
304094,0x0,US,US,0,3,1,n/a,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:46:10 10.1.0.2 1,2016/11/15 08:46:10,001801 015967,TRAFFIC,end,1,2016/11 /15
08:46:10,64.85.77.6,50.2 32.155.145,64.85.77.6,10.250 .0.10,inbound-web-browsing,, ,web-
browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15
08:46:10,41776,1,42156,80,42 156,80,0x40001c,tcp,allow,89 147,10971,78176,110,2016/11/
15 08:45:50,4,government,0,2 816304057,0x0,US,US,0,51,59, tcp-rst-from-client,0,0,0,0, ,ATL-
PAN-01,from-policy
Nov 15 08:46:08 10.1.0.2 1,2016/ 11/15 08:46:08,001801015967, TRAFFIC,start,1,2016/11/15
0 8:46:08,64.85.77.2,50.232.15 5.145,64.85.77.2,10.250.0.10 ,inbound-web-browsing,,,web-
browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell- secureworks,2016/11/15
08:46 :08,40469,1,60485,80,60485,8 0,0x400000,tcp,allow,684,610 ,74,4,2016/11/15
08:46:07,0, any,0,2816303826,0x0,US,US,0 ,3,1,n/a,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:46:08 10.1.0.2 1,2016/11/15 08:46 :08,001801015967,TRAFFIC,end ,1,2016/11/15
08:46:08,64.85 .97.253,50.232.155.145,64.85 .97.253,10.250.0.10,inbound- web-
browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-securewor
ks,2016/11/15 08:46:08,41169 ,1,54453,80,54453,80,0x40001 c,tcp,allow,97812,13496,8431
6,154,2016/11/15 08:45:22,30 ,government,0,2816303860,0x0 ,US,US,0,87,67,tcp-
fin,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:46:08 10.1.0.2 1,20 16/11/15 08:46:08,0018010159 67,TRAFFIC,end,1,2016/11/15
08:46:08,12.206.16.210,50.23 2.155.145,12.206.16.210,10.2 50.0.10,inbound-
web-browsing ,,,incomplete,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-
secureworks,2016/11/15 08:46:08,36962,1,52443,80,52 443,80,0x40001b,tcp,allow,31
2,186,126,5,2016/11/15 08:45 :47,5,any,0,2816303882,0x0,U S,US,0,3,2,tcp-rst-from-serv
er,0,0,0,0,,ATL-PAN-01,from- policy
Nov 15 08:46:08 10.1. 0.2 1,2016/11/15 08:46:08,00 1801015967,TRAFFIC,start,1,2
016/11/15 08:46:08,66.192.63 .2,50.232.155.145,66.192.63. 2,10.250.0.10,inbound-web-br
owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201
6/11/15 08:46:08,256012,1,30 379,80,30379,80,0x400000,tcp ,allow,1523,1449,74,4,2016/1
1/15 08:46:08,0,any,0,281630 3950,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:07 10.1.0.2 1, 2016/11/15 08:46:07,00180101 5967,TRAFFIC,end,1,2016/11/1
5 08:46:07,64.85.77.5,50.232 .155.145,64.85.77.5,10.250.0 .10,inbound-web-browsing,,,w
eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15
08 :46:07,32885,1,45472,80,4547 2,80,0x40001c,tcp,allow,4076 ,1730,2346,15,2016/11/15

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

08: 45:50,1,government,0,2816303 741,0x0,US,US,0,10,5,tcp-rst -from-client,0,0,0,0,,ATL-PA
N-01,from-policy
Nov 15 08:4 6:07 10.1.0.2 1,2016/11/15 0 8:46:07,001801015967,TRAFFIC ,end,1,2016/11/15
08:46:07,1 52.133.7.129,50.232.155.145, 152.133.7.129,10.250.0.10,in bound-
web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-
sec ureworks,2016/11/15 08:46:07 ,40229,1,61684,80,61684,80,0
x40001a,tcp,allow,20171,5824 ,14347,28,2016/11/15 08:45:4 7,4,government,0,2816303750,
0x0,US,US,0,13,15,tcp-rst-fr om-client,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:46:0 6 10.1.0.2 1,2016/11/15 08:4 6:06,001801015967,TRAFFIC,st art,1,2016/11/15
08:46:06,64 .85.77.14,50.232.155.145,64. 85.77.14,10.250.0.10,inbound -web-browsing,,,web-
browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15
08:46:06,3679 0,1,33344,80,33344,80,0x4000 00,tcp,allow,689,615,74,4,20 16/11/15
08:46:05,1,any,0,28 16303706,0x0,US,US,0,3,1,n/a ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:46:06 10.1.0. 2 1,2016/11/15 08:46:06,0018 01015967,TRAFFIC,start,1,201
6/11/15 08:46:06,216.212.116 .58,50.232.155.145,216.212.1 16.58,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-
secureworks ,2016/11/15 08:46:06,26601,1 ,3699,80,3699,80,0x400000,tc
p,allow,694,632,62,4,2016/11 /15 08:46:05,0,any,0,2816303 626,0x0,US,US,0,3,1,n/a,0,0,
0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:06 10.1.0.2 1,2 016/11/15 08:46:06,001801015 967,TRAFFIC,end,1,2016/11/15
08:46:06,64.85.77.6,50.232. 155.145,64.85.77.6,10.250.0. 10,inbound-web-browsing,,,we
b-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08:
46:06,44987,1,50626,80,50626 ,80,0x40001c,tcp,allow,37287 ,7502,29785,48,2016/11/15
08 :45:46,4,government,0,281630 3691,0x0,US,US,0,25,23,tcp-f in,0,0,0,0,,ATL-PAN-01,from-
policy
Nov 15 08:46:06 10.1. 0.2 1,2016/11/15 08:46:06,00 1801015967,TRAFFIC,start,1,2
016/11/15 08:46:06,64.85.97. 241,50.232.155.145,64.85.97. 241,10.250.0.10,inbound-web-
browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2
016/11/15 08:46:06,42014,1,5 6713,80,56713,80,0x400000,tc p,allow,693,619,74,4,2016/11 /15
08:46:05,0,any,0,2816303 704,0x0,US,US,0,3,1,n/a,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:06 10.1.0.2 1,2 016/11/15 08:46:06,001801015 967,TRAFFIC,end,1,2016/11/15
08:46:06,64.85.77.12,50.232 .155.145,64.85.77.12,10.250. 0.10,inbound-web-browsing,,,
incomplete,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08:

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

46:06,234727,1,46073,80,4607 3,80,0x40001b,tcp,allow,340, 206,134,5,2016/11/15 08:45:5
0,0,any,0,2816303635,0x0,US, US,0,3,2,tcp-rst-from-server ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:46:06 10.1.0. 2 1,2016/11/15 08:46:06,0018 01015967,TRAFFIC,start,1,201
6/11/15 08:46:06,216.212.116 .58,50.232.155.145,216.212.1 16.58,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-
secureworks ,2016/11/15 08:46:06,53457,1 ,3701,80,3701,80,0x400000,tc
p,allow,695,633,62,4,2016/11 /15 08:46:05,1,any,0,2816303 705,0x0,US,US,0,3,1,n/a,0,0,
0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:04 10.1.0.2 1,2 016/11/15 08:46:04,001801015 967,TRAFFIC,end,1,2016/11/15
08:46:04,152.133.7.129,50.2 32.155.145,152.133.7.129,10. 250.0.10,inbound-web-browsin
g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15
08:46:04,48143,1,11683,80 ,11683,80,0x40001a,tcp,allow ,4266,2627,1639,9,2016/11/15
08:45:48,0,government,0,281 6303489,0x0,US,US,0,5,4,tcp- rst-from-client,0,0,0,0,,ATL -
PAN-01,from-policy
Nov 15 0 8:46:03 10.1.0.2 1,2016/11/1 5 08:46:03,001801015967,TRAF FIC,start,1,2016/11/15
08:46 :03,12.48.151.106,50.232.155 .145,12.48.151.106,10.250.0. 10,inbound-
web-browsing,,,we b-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-
secureworks,2016/11/15 08: 46:03,50004,1,45632,80,45632 ,80,0x400000,tcp,allow,639,5
73,66,4,2016/11/15 08:46:03, 0,any,0,2816303461,0x0,US,US ,0,3,1,n/a,0,0,0,0,,ATL-PAN-
01,from-policy
Nov 15 08:46: 03 10.1.0.2 1,2016/11/15 08: 46:03,001801015967,TRAFFIC,e nd,1,2016/11/15
08:46:03,64. 85.77.5,50.232.155.145,64.85 .77.5,10.250.0.10,inbound-we b-browsing,,,web-
browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-secureworks ,2016/11/15
08:46:03,33818,1 ,50600,80,50600,80,0x40001c, tcp,allow,39066,7810,31256,4 9,2016/11/15
08:45:28,19,gov ernment,0,2816303440,0x0,US, US,0,25,24,tcp-rst-from-clie nt,0,0,0,0,,ATL-
PAN-01,from- policy
Nov 15 08:46:03 10.1. 0.2 1,2016/11/15 08:46:03,00 1801015967,TRAFFIC,start,1,2
016/11/15 08:46:03,12.48.151 .106,50.232.155.145,12.48.15 1.106,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-
secureworks ,2016/11/15 08:46:03,25170,1 ,57573,80,57573,80,0x400000,
tcp,allow,736,670,66,4,2016/ 11/15 08:46:03,0,any,0,28163 03460,0x0,US,US,0,3,1,n/a,0,
0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:46:03 10.1.0.2 1 ,2016/11/15 08:46:03,0018010 15967,TRAFFIC,start,1,2016/1
1/15 08:46:03,12.48.151.106, 50.232.155.145,12.48.151.106 ,10.250.0.10,inbound-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:46:03,26270,1,3978 4,80,39784,80,0x400000,tcp,allow,519,453,66,4,2016/11/15 08:46:02,1,any,0,2816303454 ,0x0,US,US,0,3,1,n/a,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:46:03 10.1.0.2 1,2016 /11/15 08:46:03,001801015967 ,TRAFFIC,end,1,2016/11/15 08 :46:03,207.99.81.78,50.232.1 55.145,207.99.81.78,10.250.0 .10,inbound-web-browsing,,,web-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15 08 :46:03,61361,1,2619,80,2619, 80,0x40001a,tcp,allow,2341,7 66,1575,8,2016/11/15 08:45:47,0,government,0,2816303439, 0x0,US,US,0,5,3,tcp-rst-from -client,0,0,0,0,,ATL-PAN-01, from-policy
Nov 15 08:46:03 10.1.0.2 1,2016/11/15 08:46: 03,001801015967,TRAFFIC,star t,1,2016/11/15 08:46:03,12.4 8.151.106,50.232.155.145,12. 48.151.106,10.250.0.10,inbou nd-web-browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure works,2016/11/15 08:46:03,41 687,1,37651,80,37651,80,0x40 0000,tcp,allow,709,643,66,4, 2016/11/15 08:46:03,0,any,0, 2816303459,0x0,US,US,0,3,1,n /a,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:00 10.1. 0.2 1,2016/11/15 08:46:00,00 1801015967,TRAFFIC,start,1,2 016/11/15 08:46:00,64.85.97. 171,50.232.155.145,64.85.97. 171,10.250.0.10,inbound-web-browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2 016/11/15 08:46:00,38529,1,5 0050,80,50050,80,0x400000,tc p,allow,618,544,74,4,2016/11 /15 08:46:00,0,any,0,2816303 215,0x0,US,US,0,3,1,n/a,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:46:01 10.1.0.2 1,2 016/11/15 08:46:01,001801015 967,TRAFFIC,end,1,2016/11/15 08:46:01,64.85.77.8,50.232. 155.145,64.85.77.8,10.250.0. 10,inbound-web-browsing,,,web-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08: 46:01,18952,1,52211,80,52211 ,80,0x40001c,tcp,allow,73340 ,12702,60638,98,2016/11/15 0 8:43:45,120,government,0,281 6303255,0x0,US,US,0,49,49,tc p-fin,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:46:02 10 .1.0.2 1,2016/11/15 08:46:02 ,001801015967,TRAFFIC,end,1, 2016/11/15 08:46:02,52.1.7.1 01,50.232.155.145,52.1.7.101 ,10.250.0.10,inbound-web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:46:02,259648,1,498 01,80,49801,80,0x40001a,tcp, allow,55046,9292,45754,67,20 16/11/15 08:45:08,38,governm ent,0,2816303309,0x0,US,US,0 ,31,36,tcp-rst-from-client,0 ,0,0,0,,ATL-PAN-01,from-poli cy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:46:00 10.1.0.2 1,2016/11/15 08:46:00,001801 015967,TRAFFIC,start,1,2016/ 11/15 08:46:00,209.67.78.51, 50.232.155.145,209.67.78.51, 10.250.0.10,inbound-web-brow sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/ 11/15 08:46:00,53728,1,36716 ,80,36716,80,0x400000,tcp,al low,684,610,74,4,2016/11/15 08:46:00,0,any,0,2816303219, 0x0,US,US,0,3,1,n/a,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:46:02 10.1.0.2 1,2016/ 11/15 08:46:02,001801015967, TRAFFIC,end,1,2016/11/15 08: 46:02,64.85.77.6,50.232.155. 145,64.85.77.6,10.250.0.10,i nbound-web-browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15 08:46:0 2,27391,1,54080,80,54080,80, 0x40001c,tcp,allow,2050,1358 ,692,12,2016/11/15 08:45:24, 22,government,0,2816303308,0 x0,US,US,0,8,4,tcp-fin,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:46:02 10.1.0.2 1,20 16/11/15 08:46:02,0018010159 67,TRAFFIC,end,1,2016/11/15 08:46:02,52.1.7.101,50.232.1 55.145,52.1.7.101,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4 6:02,49327,1,49802,80,49802, 80,0x40001a,tcp,allow,19691, 2267,17424,28,2016/11/15 08: 45:08,38,government,0,281630 3369,0x0,US,US,0,14,14,tcp-r st-from-client,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08 :46:02 10.1.0.2 1,2016/11/15 08:46:02,001801015967,TRAFF IC,end,1,2016/11/15 08:46:02 ,64.85.77.14,50.232.155.145, 64.85.77.14,10.250.0.10,inbo und-web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:46:02,3 8455,1,40351,80,40351,80,0x4 0001c,tcp,allow,38360,3819,3 4541,54,2016/11/15 08:44:51, 55,government,0,2816303347,0 x0,US,US,0,27,27,tcp-rst-fro m-client,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:46:02 10.1.0.2 1,2016/11/15 08:46 :02,001801015967,TRAFFIC,end ,1,2016/11/15 08:46:02,152.1 33.7.129,50.232.155.145,152. 133.7.129,10.250.0.10,inboun d-web-browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew orks,2016/11/15 08:46:02,195 28,1,61683,80,61683,80,0x400 01a,tcp,allow,51927,13771,38 156,57,2016/11/15 08:45:37,9 ,government,0,2816303363,0x0 ,US,US,0,24,33,tcp-rst-from-client,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:45:59 1 0.1.0.2 1,2016/11/15 08:45:5 9,001801015967,TRAFFIC,start ,1,2016/11/15 08:45:59,12.20 6.16.210,50.232.155.145,12.2 06.16.210,10.250.0.10,inboun d-web-browsing,,,web-browsin g,vsys1,outside,dmz,ethernet 1/4,ethernet1/2,dell-securew orks,2016/11/15 08:45:59,249 85,1,52446,80,52446,80,0x400 000,tcp,allow,734,668,66,4,2 016/11/15 08:45:59,0,any,0,2 816303151,0x0,US,US,0,3,1,n/ a,0,0,0,0,,ATL-PAN-01,from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:45:59 10.1.0 .2 1,2016/11/15 08:45:59,001 801015967,TRAFFIC,start,1,20
16/11/15 08:45:59,12.206.16. 210,50.232.155.145,12.206.16 .210,10.250.0.10,inbound-web
-browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks,
2016/11/15 08:45:59,50726,1, 52445,80,52445,80,0x400000,t cp,allow,643,577,66,4,2016/1
1/15 08:45:57,2,any,0,281630 3136,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:45:59 10.1.0.2 1, 2016/11/15 08:45:59,00180101 5967,TRAFFIC,start,1,2016/11 /15
08:45:59,64.85.97.192,50 .232.155.145,64.85.97.192,10 .250.0.10,inbound-web-browsi
ng,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15
08:45:59,48096,1,60298,8 0,60298,80,0x400000,tcp,allo w,630,556,74,4,2016/11/15
08 :45:59,0,any,0,2816303160,0x 0,US,US,0,3,1,n/a,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:45:58 10.1.0.2 1,2016/11 /15 08:45:58,001801015967,TR AFFIC,start,1,2016/11/15
08: 45:58,207.99.81.78,50.232.15 5.145,207.99.81.78,10.250.0. 10,inbound-web-browsing,,,we
b-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08:
45:58,37563,1,2620,80,2620,8 0,0x400000,tcp,allow,691,629 ,62,4,2016/11/15 08:45:58,0,
any,0,2816303040,0x0,US,US,0 ,3,1,n/a,0,0,0,0,,ATL-PAN-01 ,from-policy
Nov 15 08:45:59 10.1.0.2 1,2016/11/15 08:45 :59,001801015967,TRAFFIC,sta rt,1,2016/11/15
08:45:59,64. 85.77.2,50.232.155.145,64.85 .77.2,10.250.0.10,inbound-we b-browsing,,,web-
browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-secureworks ,2016/11/15
08:45:59,53071,1 ,60410,80,60410,80,0x400000, tcp,allow,684,610,74,4,2016/ 11/15
08:45:58,1,any,0,28163 03126,0x0,US,US,0,3,1,n/a,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:45:59 10.1.0.2 1 ,2016/11/15 08:45:59,0018010 15967,TRAFFIC,end,1,2016/11/
15 08:45:59,50.246.9.145,50. 232.155.145,50.246.9.145,10. 250.0.10,inbound-web-browsin
g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15
08:45:59,21070,1,49989,80 ,49989,80,0x40001c,tcp,allow ,3165,1580,1585,9,2016/11/15
08:44:28,75,government,0,28 16303081,0x0,US,US,0,6,3,tcp -fin,0,0,0,0,,ATL-PAN-01,fro m-
policy
Nov 15 08:45:58 10. 1.0.2 1,2016/11/15 08:45:58, 001801015967,TRAFFIC,start,1 ,2016/11/15
08:45:58,67.198. 62.57,50.232.155.145,67.198. 62.57,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-
secureworks ,2016/11/15 08:45:58,38502,1 ,61295,80,61295,80,0x400000,
tcp,allow,681,615,66,4,2016/ 11/15 08:45:58,0,any,0,28163 03034,0x0,US,US,0,3,1,n/a,0,
0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:45:59 10.1.0.2 1 ,2016/11/15 08:45:59,0018010 15967,TRAFFIC,end,1,2016/11/
15 08:45:59,50.246.9.145,50. 232.155.145,50.246.9.145,10. 250.0.10,inbound-web-browsin

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

g,,,incomplete,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15 08:45:59,40011,1,35848,80,3 5848,80,0x40001b,tcp,allow,3 12,186,126,5,2016/11/15 08:4 4:28,75,any,0,2816303095,0x0 ,US,US,0,3,2,tcp-rst-from-se rver,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:45:59 10. 1.0.2 1,2016/11/15 08:45:59, 001801015967,TRAFFIC,drop,1, 2016/11/15 08:45:59,220.134. 223.89,50.232.155.145,0.0.0. 0,0.0.0.0,deny-remaining,,,n ot-applicable,vsys1,outside, dmz,ethernet1/4,,dell-secure works,2016/11/15 08:45:59,0, 1,19464,23,0,0,0x0,tcp,deny, 60,60,0,1,2016/11/15 08:45:5 8,0,any,0,2816303124,0x0,TW, US,0,1,0,policy-deny,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:45:58 10.1.0.2 1,2016 /11/15 08:45:58,001801015967 ,TRAFFIC,start,1,2016/11/15 08:45:58,67.198.62.57,50.232 .155.145,67.198.62.57,10.250 .0.10,inbound-web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15 08:45:58,4904,1,61294,80,612 94,80,0x400000,tcp,allow,638 ,572,66,4,2016/11/15 08:45:5 7,1,any,0,2816303030,0x0,US, US,0,3,1,n/a,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 5:56 10.1.0.2 1,2016/11/15 0 8:45:56,001801015967,TRAFFIC ,drop,1,2016/11/15 08:45:56, 112.166.168.249,50.232.155.1 45,0.0.0.0,0.0.0.0,deny-rema ining,,,not-applicable,vsys1 ,outside,dmz,ethernet1/4,,de ll-secureworks,2016/11/15 08 :45:56,0,1,48575,23,0,0,0x0, tcp,deny,60,60,0,1,2016/11/1 5 08:45:55,0,any,0,2816302775,0x0,KR,US,0,1,0,policy-den y,0,0,0,0,,ATL-PAN-01,from-p olicy
Nov 15 08:45:54 10.1.0 .2 1,2016/11/15 08:45:54,001 801015967,TRAFFIC,end,1,2016 /11/15 08:45:54,66.192.63.2, 50.232.155.145,66.192.63.2,1 0.250.0.10,inbound-web-brows ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15 08:45:54,38960,1,57064, 80,57064,80,0x40001c,tcp,all ow,5874,2792,3082,12,2016/11 /15 08:44:02,96,government,0 ,2816302503,0x0,US,US,0,8,4, tcp-fin,0,0,0,0,,ATL-PAN-01, from-policy
Nov 15 08:45:54 10.1.0.2 1,2016/11/15 08:45: 54,001801015967,TRAFFIC,end, 1,2016/11/15 08:45:54,152.13 3.7.129,50.232.155.145,152.1 33.7.129,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:45:54,1924 1,1,36196,80,36196,80,0x4000 1a,tcp,allow,89709,9412,8029 7,104,2016/11/15 08:45:20,18 ,government,0,2816302525,0x0 ,US,US,0,41,63,tcp-rst-from-client,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:45:54 1 0.1.0.2 1,2016/11/15 08:45:5 4,001801015967,TRAFFIC,start ,1,2016/11/15 08:45:54,104.1 29.204.75,50.232.155.145,104 .129.204.75,10.250.0.10,inbo und-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:45:54,2 5493,1,40443,80,40443,80,0x4 00000,tcp,allow,1171,1097,74 ,4,2016/11/15 08:45:54,0,any ,0,2816302572,0x0,US,US,0,3, 1,n/a,0,0,0,0,,ATL-PAN-01,fr om-policy
Nov 15 08:45:54 10 .1.0.2 1,2016/11/15 08:45:54 ,001801015967,TRAFFIC,start, 1,2016/11/15 08:45:54,104.12 9.204.75,50.232.155.145,104. 129.204.75,10.250.0.10,inbou nd-web-browsing,,,web-browsi ng,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell-secure works,2016/11/15 08:45:54,36 279,1,40444,80,40444,80,0x40 0000,tcp,allow,1182,1108,74, 4,2016/11/15 08:45:54,0,any, 0,2816302573,0x0,US,US,0,3,1 ,n/a,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:45:53 10. 1.0.2 1,2016/11/15 08:45:53, 001801015967,TRAFFIC,start,1 ,2016/11/15 08:45:53,66.192. 63.2,50.232.155.145,66.192.6 3.2,10.250.0.10,inbound-web- browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2 016/11/15 08:45:53,29192,1,1 2667,80,12667,80,0x400000,tc p,allow,1523,1449,74,4,2016/ 11/15 08:45:52,1,any,0,28163 02454,0x0,US,US,0,3,1,n/a,0, 0,0,0,,ATL-PAN-01,from-polic y
Nov 15 08:45:53 10.1.0.2 1 ,2016/11/15 08:45:53,0018010 15967,TRAFFIC,end,1,2016/11/ 15 08:45:53,152.133.7.129,50 .232.155.145,152.133.7.129,1 0.250.0.10,inbound-web-brows ing,,,web-browsing,vsys1,out side,dmz,ethernet1/4,etherne t1/2,dell-secureworks,2016/1 1/15 08:45:53,38328,1,12817, 80,12817,80,0x40001a,tcp,all ow,17034,5711,11323,23,2016/ 11/15 08:45:33,4,government, 0,2816302402,0x0,US,US,0,12, 11,tcp-rst-from-client,0,0,0 ,0,,ATL-PAN-01,from-policy
N ov 15 08:45:52 10.1.0.2 1,20 16/11/15 08:45:52,0018010159 67,TRAFFIC,end,1,2016/11/15 08:45:52,68.184.179.22,50.23 2.155.145,68.184.179.22,10.2 50.0.10,inbound-web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5 08:45:52,32101,1,59171,80, 59171,80,0x40001c,tcp,allow, 2338,753,1585,9,2016/11/15 0 8:43:40,116,government,0,281 6302247,0x0,US,US,0,6,3,tcp-fin,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:45:52 10.1 .0.2 1,2016/11/15 08:45:52,0 01801015967,TRAFFIC,start,1, 2016/11/15 08:45:52,64.85.97 .172,50.232.155.145,64.85.97 .172,10.250.0.10,inbound-web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15 08:45:52,57048,1, 37948,80,37948,80,0x400000,t cp,allow,684,610,74,4,2016/1 1/15 08:45:52,0,any,0,281630 2340,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:45:52 10.1.0.2 1, 2016/11/15 08:45:52,00180101 5967,TRAFFIC,end,1,2016/11/1 5 08:45:52,68.184.179.22,50. 232.155.145,68.184.179.22,10 .250.0.10,inbound-web-browsi

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

ng,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15 08:45:52,26489,1,59169,8 0,59169,80,0x40001c,tcp,allo w,31231,1690,29541,39,2016/1 1/15 08:43:40,116,government ,0,2816302246,0x0,US,US,0,16 ,23,tcp-fin,0,0,0,0,,ATL-PAN -01,from-policy
Nov 15 08:45 :51 10.1.0.2 1,2016/11/15 08 :45:51,001801015967,TRAFFIC, end,1,2016/11/15 08:45:51,10 8.66.253.68,50.232.155.145,1 08.66.253.68,10.250.0.10,inb ound-web-browsing,,,incomple te,vsys1,outside,dmz,etherne t1/4,ethernet1/2,dell- secure works,2016/11/15 08:45:51,40 376,1,60733,80,60733,80,0x40 001b,tcp,allow,312,186,126,5 ,2016/11/15 08:45:23,12,any, 0,2816302223,0x0,US,US,0,3,2 ,tcp-rst-from-server,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:45:51 10.1.0.2 1,2016 /11/15 08:45:51,001801015967 ,TRAFFIC,end,1,2016/11/15 08 :45:51,50.246.9.145,50.232.1 55.145,50.246.9.145,10.250.0 .10,inbound-web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15 08 :45:51,27811,1,59271,80,5927 1,80,0x40001a,tcp,allow,1628 0,3385,12895,27,2016/11/15 0 8:45:35,0,government,0,28163 02156,0x0,US,US,0,14,13,tcp- rst-from-client,0,0,0,0,,ATL - PAN-01,from-policy
Nov 15 0 8:45:51 10.1.0.2 1,2016/11/1 5 08:45:51,001801015967,TRAF FIC,end,1,2016/11/15 08:45:5 1,108.66.253.68,50.232.155.1 45,108.66.253.68,10.250.0.10 ,inbound- web-browsing,,,web- browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell- secureworks,2016/11/15 08:45 :51,19493,1,60730,80,60730,8 0,0x40001c,tcp,allow,113803, 10375,103428,120,2016/11/15 08:45:22,13,government,0,281 6302179,0x0,US,US,0,45,75,tc p-rst-from-client,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:45:51 10.1.0.2 1,2016/11 /15 08:45:51,001801015967,TR AFFIC,end,1,2016/11/15 08:45 :51,108.66.253.68,50.232.155 .145,108.66.253.68,10.250.0. 10,inbound- web-browsing,,,in complete,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell- secureworks,2016/11/15 08:45 :51,45716,1,60732,80,60732,8 0,0x40001b,tcp,allow,312,186 ,126,5,2016/11/15 08:45:23,1 2,any,0,2816302187,0x0,US,US ,0,3,2,tcp-rst-from-server,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:45:51 10.1.0.2 1,2016/11/15 08:45:51,001801 015967,TRAFFIC,end,1,2016/11 /15 08:45:51,108.66.253.68,5 0.232.155.145,108.66.253.68, 10.250.0.10,inbound-web-brow sing,,,incomplete,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15 08:45:51,44920,1,60731,8 0,60731,80,0x40001b,tcp,allo w,312,186,126,5,2016/11/15 0 8:45:22,13,any,0,2816302217, 0x0,US,US,0,3,2,tcp-rst-from -server,0,0,0,0,,ATL-PAN-01, from-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:45:50 10.1.0.2 1,2016/11/15 08:45: 50,001801015967,TRAFFIC,star t,1,2016/11/15 08:45:50,64.8 5.77.6,50.232.155.145,64.85. 77.6,10.250.0.10,inbound-web -browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks, 2016/11/15 08:45:50,41776,1, 42156,80,42156,80,0x400000,t cp,allow,684,610,74,4,2016/1 1/15 08:45:50,0,any,0,281630 2142,0x0,US,US,0,3,1,n/a,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:45:50 10.1.0.2 1, 2016/11/15 08:45:50,00180101 5967,TRAFFIC,end,1,2016/11/1 5 08:45:50,76.125.21.93,50.2 32.155.145,76.125.21.93,10.2 50.0.10,inbound-web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5 08:45:50,43110,1,52844,80, 52844,80,0x40001c,tcp,allow, 31123,1202,29921,40,2016/11/ 15 08:45:13,21,government,0, 2816302104,0x0,US,US,0,12,28 ,tcp-rst-from-server,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:45:50 10.1.0.2 1,2016 /11/15 08:45:50,001801015967 ,TRAFFIC,start,1,2016/11/15 08:45:50,64.85.77.5,50.232.1 55.145,64.85.77.5,10.250.0.1 0,inbound-web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -secureworks,2016/11/15 08:4 5:50,32885,1,45472,80,45472, 80,0x400000,tcp,allow,703,62 9,74,4,2016/11/15 08:45:50,0 ,any,0,2816302132,0x0,US,US, 0,3,1,n/a,0,0,0,0,,ATL-PAN-0 1,from-policy
Nov 15 08:45:5 0 10.1.0.2 1,2016/11/15 08:4 5:50,001801015967,TRAFFIC,en d,1,2016/11/15 08:45:50,173. 14.221.37,50.232.155.145,173 .14.221.37,10.250.0.10,inbou nd-web-browsing,,,incomplete ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:45:50,3289 3,1,62534,80,62534,80,0x4000 1b,tcp,allow,438,246,192,7,2 016/11/15 08:44:44,50,any,0, 2816302084,0x0,US,US,0,4,3,t cp-rst-from-server,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:45:50 10.1.0.2 1,2016/1 1/15 08:45:50,001801015967,T RAFFIC,start,1,2016/11/15 08 :45:50,209.67.78.55,50.232.1 55.145,209.67.78.55,10.250.0 .10,inbound-web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15 08 :45:50,249448,1,38727,80,387 27,80,0x400000,tcp,allow,693 ,619,74,4,2016/11/15 08:45:5 0,0,any,0,2816302136,0x0,US, US,0,3,1,n/a,0,0,0,0,,ATL-PA N-01,from-policy
Nov 15 08:4 5:49 10.1.0.2 1,2016/11/15 0 8:45:49,001801015967,TRAFFIC ,end,1,2016/11/15 08:45:49,1 52.133.7.129,50.232.155.145, 152.133.7.129,10.250.0.10,in bound-web-browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec ureworks,2016/11/15 08:45:49 ,20162,1,61682,80,61682,80,0 x40001a,tcp,allow,4266,2627, 1639,9,2016/11/15 08:45:33,0 ,government,0,2816302023,0x0 ,US,US,0,5,4,tcp-rst-from-cl ient,0,0,0,0,,ATL-PAN-01,fro m-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:45:49 10. 1.0.2 1,2016/11/15 08:45:49, 001801015967,TRAFFIC,end,1,2
016/11/15 08:45:49,152.133.7 .129,50.232.155.145,152.133. 7.129,10.250.0.10,inbound-
we b-browsing,,,web-browsing,vs ys1,outside,dmz,ethernet1/4, ethernet1/2,dell-
secureworks ,2016/11/15 08:45:49,4965,1, 17822,80,17822,80,0x40001c,t
cp,allow,4446,2747,1699,12,2 016/11/15 08:45:33,0,governm
ent,0,2816302057,0x0,US,US,0 ,7,5,tcp-rst-from-client,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:45:49 10.1.0.2 1, 2016/11/15 08:45:49,00180101 5967,TRAFFIC,start,1,2016/11 /15
08:45:49,152.133.7.129,5 0.232.155.145,152.133.7.129, 10.250.0.10,inbound-web-brow
sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/
11/15 08:45:49,48143,1,11683 ,80,11683,80,0x400000,tcp,al low,1606,1540,66,4,2016/11/1 5
08:45:48,0,any,0,281630200 1,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:45:49 10.1.0.2 1,201 6/11/15 08:45:49,00180101596 7,TRAFFIC,start,1,2016/11/15
08:45:49,152.133.7.129,50.2 32.155.145,152.133.7.129,10. 250.0.10,inbound-web-browsin
g,,,web-browsing,vsys1,outsi de,dmz,ethernet1/4,ethernet1 /2,dell-secureworks,2016/11/ 15
08:45:49,31653,1,61685,80 ,61685,80,0x400000,tcp,allow ,1606,1540,66,4,2016/11/15 0
8:45:47,1,any,0,2816302000,0 x0,US,US,0,3,1,n/a,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:45:48 10.1.0.2 1,2016/1 1/15 08:45:48,001801015967,T RAFFIC,start,1,2016/11/15
08 :45:48,152.133.7.129,50.232. 155.145,152.133.7.129,10.250 .0.10,inbound-
web-browsing,, ,web-browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-
secureworks,2016/11/15 08:45:48,40229,1,61684,80,61 684,80,0x400000,tcp,allow,16
06,1540,66,4,2016/11/15 08:4 5:47,0,any,0,2816301988,0x0, US,US,0,3,1,n/a,0,0,0,0,,ATL -
PAN-01,from-policy
Nov 15 0 8:45:48 10.1.0.2 1,2016/11/1 5 08:45:48,001801015967,TRAF FIC,end,1,2016/11/15
08:45:4 8,66.192.63.2,50.232.155.145 ,66.192.63.2,10.250.0.10,inb ound-web-browsing,,,web-
brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu reworks,2016/11/15 08:45:48,
27239,1,42257,80,42257,80,0x 40001c,tcp,allow,75893,16858 ,59035,67,2016/11/15 08:44:2
4,68,government,0,2816301943 ,0x0,US,US,0,24,43,tcp-fin,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:45:47 10.1.0.2 1,2016/11/15 08:45:47,001801 015967,TRAFFIC,start,1,2016/
11/15 08:45:47,207.99.81.78, 50.232.155.145,207.99.81.78, 10.250.0.10,inbound-web-brow
sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/
11/15 08:45:47,61361,1,2619, 80,2619,80,0x400000,tcp,allo w,708,646,62,4,2016/11/15
08 :45:47,0,any,0,2816301919,0x 0,US,US,0,3,1,n/a,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:45:46 10.1.0.2 1,2016/11 /15 08:45:46,001801015967,TR AFFIC,start,1,2016/11/15
08: 45:46,208.87.238.180,50.232. 155.145,208.87.238.180,10.25 0.0.10,inbound-

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15 08:45:46,13399,1,35678,80,3 5678,80,0x400000,tcp,allow,8 68,802,66,4,2016/11/15 08:45 :46,0,any,0,2816301765,0x0,U S,US,0,3,1,n/a,0,0,0,0,,ATL-PAN-01,from-policy
Nov 15 08 :45:46 10.1.0.2 1,2016/11/15 08:45:46,001801015967,TRAFF IC,start,1,2016/11/15 08:45: 46,64.85.77.6,50.232.155.145 ,64.85.77.6,10.250.0.10,inbo und-web-browsing,,,web-brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:45:46,4 4987,1,50626,80,50626,80,0x4 00000,tcp,allow,684,610,74,4 ,2016/11/15 08:45:46,0,any,0 ,2816301826,0x0,US,US,0,3,1, n/a,0,0,0,0,,ATL-PAN-01,from -policy
Nov 15 08:45:47 10.1 .0.2 1,2016/11/15 08:45:47,0 01801015967,TRAFFIC,start,1, 2016/11/15 08:45:47,64.85.77 .8,50.232.155.145,64.85.77.8 ,10.250.0.10,inbound-web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-secureworks,2016 /11/15 08:45:47,49108,1,3462 6,80,34626,80,0x400000,tcp,a llow,650,576,74,4,2016/11/15 08:45:46,0,any,0,2816301907 ,0x0,US,US,0,3,1,n/a,0,0,0,0 ,,ATL-PAN-01,from-policy
Nov 15 08:45:45 10.1.0.2 1,2016 /11/15 08:45:45,001801015967 ,TRAFFIC,start,1,2016/11/15 08:45:45,152.133.7.129,50.23 2.155.145,152.133.7.129,10.2 50.0.10,inbound-web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-secureworks,2016/11/1 5 08:45:45,19528,1,61683,80, 61683,80,0x400000,tcp,allow, 1606,1540,66,4,2016/11/15 08 :45:37,8,any,0,2816301679,0x 0,US,US,0,3,1,n/a,0,0,0,0,,A TL-PAN-01,from-policy
Nov 15 08:45:45 10.1.0.2 1,2016/11 /15 08:45:45,001801015967,TR AFFIC,start,1,2016/11/15 08: 45:45,64.85.77.2,50.232.155. 145,64.85.77.2,10.250.0.10,i nbound-web-browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se cureworks,2016/11/15 08:45:4 5,29536,1,60310,80,60310,80, 0x400000,tcp,allow,684,610,7 4,4,2016/11/15 08:45:45,0,an y,0,2816301667,0x0,US,US,0,3 ,1,n/a,0,0,0,0,,ATL-PAN-01,f rom-policy
Nov 15 08:45:44 1 0.1.0.2 1,2016/11/15 08:45:4 4,001801015967,TRAFFIC,end,1 ,2016/11/15 08:45:44,64.179. 192.42,50.232.155.145,64.179 .192.42,10.250.0.10,inbound- web-browsing,,,web-browsing, vsys1,outside,dmz,ethernet1/ 4,ethernet1/2,dell-securewor ks,2016/11/15 08:45:44,38421 ,1,13709,80,13709,80,0x40001 c,tcp,allow,1727,1336,391,9, 2016/11/15 08:43:29,119,gove rnment,0,2816301532,0x0,US,U S,0,6,3,tcp-fin,0,0,0,0,,ATL - PAN-01,from-policy
Nov 15 0 8:45:44 10.1.0.2 1,2016/11/1 5 08:45:44,001801015967,TRAF FIC,end,1,2016/11/15 08:45:4 4,216.81.81.80,50.232.155.14 5,216.81.81.80,10.250.0.10,i nbound-web-browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

cureworks,2016/11/15 08:45:4 4,31928,1,63669,80,63669,80, 0x40001b,tcp,allow,8155,749, 7406,13,2016/11/15 08:43:18, 130,government,0,2816301536, 0x0,US,US,0,6,7,tcp-rst-from - server,0,0,0,0,,ATL-PAN-01, from-policy
Nov 15 08:45:44 10.1.0.2 1,2016/11/15 08:45: 44,001801015967,TRAFFIC,end, 1,2016/11/15 08:45:44,64.179 .192.42,50.232.155.145,64.17 9.192.42,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:45:44,8787 ,1,16942,80,16942,80,0x40001 c,tcp,allow,1699,1309,390,9, 2016/11/15 08:43:29,119,gove rnment,0,2816301504,0x0,US,U S,0,6,3,tcp-fin,0,0,0,0,,ATL - PAN-01,from-policy
Nov 15 0 8:45:44 10.1.0.2 1,2016/11/1 5 08:45:44,001801015967,TRAF FIC,end,1,2016/11/15 08:45:4 4,64.179.192.42,50.232.155.1 45,64.179.192.42,10.250.0.10 ,inbound-web-browsing,,,web- browsing,vsys1,outside,dmz,e thernet1/4,ethernet1/2,dell-secureworks,2016/11/15 08:45 :44,11078,1,29422,80,29422,8 0,0x40001c,tcp,allow,31484,2 207,29277,46,2016/11/15 08:4 3:29,119,government,0,281630 1505,0x0,US,US,0,24,22,tcp-f in,0,0,0,0,,ATL-PAN-01,from- policy
Nov 15 08:45:44 10.1. 0.2 1,2016/11/15 08:45:44,00 1801015967,TRAFFIC,end,1,201 6/11/15 08:45:44,104.182.206 .4,50.232.155.145,104.182.20 6.4,10.250.0.10,inbound-web-browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2 016/11/15 08:45:44,29356,1,6 3213,80,63213,80,0x40001a,tc p,allow,91215,11725,79490,10 1,2016/11/15 08:44:06,82,gov ernment,0,2816301518,0x0,US, US,0,40,61,tcp-rst-from-clie nt,0,0,0,0,,ATL-PAN-01,from- policy
Nov 15 08:45:44 10.1. 0.2 1,2016/11/15 08:45:44,00 1801015967,TRAFFIC,end,1,201 6/11/15 08:45:44,64.85.77.5, 50.232.155.145,64.85.77.5,10 .250.0.10,inbound-web-browsing,,,web-browsing,vsys1,outs ide,dmz,ethernet1/4,ethernet 1/2,dell-secureworks,2016/11 /15 08:45:44,41591,1,35328,8 0,35328,80,0x40001c,tcp,allo w,5124,1766,3358,15,2016/11/ 15 08:45:18,10,government,0, 2816301528,0x0,US,US,0,10,5, tcp-fin,0,0,0,0,,ATL-PAN-01, from-policy
Nov 15 08:45:44 10.1.0.2 1,2016/11/15 08:45: 44,001801015967,TRAFFIC,end, 1,2016/11/15 08:45:44,152.13 3.7.129,50.232.155.145,152.1 33.7.129,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:45:44,3663 4,1,21003,80,21003,80,0x4000 1a,tcp,allow,56018,16287,397 31,64,2016/11/15 08:45:20,8, government,0,2816301525,0x0, US,US,0,28,36,tcp-rst-from-c lient,0,0,0,0,,ATL-PAN-01,fr om-policy

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Nov 15 08:45:44 10 .1.0.2 1,2016/11/15 08:45:44 ,001801015967,TRAFFIC,end,1,
2016/11/15 08:45:44,207.99.8 1.78,50.232.155.145,207.99.8 1.78,10.250.0.10,inbound-web
-browsing,,,web-browsing,vsy s1,outside,dmz,ethernet1/4,e thernet1/2,dell-secureworks,
2016/11/15 08:45:44,43370,1, 2616,80,2616,80,0x40001a,tcp ,allow,30611,3530,27081,41,2
016/11/15 08:44:56,32,govern ment,0,2816301521,0x0,US,US, 0,16,25,tcp-rst-from-client,
0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:45:42 10.1.0.2 1,2016/11/15 08:45:42,00180 1015967,TRAFFIC,end,1,2016/1
1/15 08:45:42,73.237.18.102, 50.232.155.145,73.237.18.102 ,10.250.0.10,inbound-
web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-
secureworks,2016 /11/15 08:45:42,29976,1,4967 6,80,49676,80,0x40001c,tcp,a
llow,26916,3167,23749,60,201 6/11/15 08:43:28,118,governm
ent,0,2816301284,0x0,US,US,0 ,29,31,tcp-fin,0,0,0,0,,ATL- PAN-01,from-policy
Nov 15 08 :45:41 10.1.0.2 1,2016/11/15 08:45:41,001801015967,TRAFF IC,end,1,2016/11/15
08:45:41 ,209.67.78.52,50.232.155.145 ,209.67.78.52,10.250.0.10,in bound-web-
browsing,,,web-bro wsing,vsys1,outside,dmz,ethe rnet1/4,ethernet1/2,dell-sec
ureworks,2016/11/15 08:45:41 ,262078,1,60155,80,60155,80, 0x40001c,tcp,allow,102099,11
477,90622,157,2016/11/15 08: 45:08,17,government,0,281630 1200,0x0,US,US,0,85,72,tcp-f
in,0,0,0,0,,ATL-PAN-01,from- policy
Nov 15 08:45:39 10.1. 0.2 1,2016/11/15 08:45:39,00 1801015967,TRAFFIC,end,1,201
6/11/15 08:45:39,50.246.9.14 5,50.232.155.145,50.246.9.14 5,10.250.0.10,inbound-web-br
owsing,,,web-browsing,vsys1, outside,dmz,ethernet1/4,ethe rnet1/2,dell-secureworks,201
6/11/15 08:45:39,33122,1,288 28,80,28828,80,0x40001a,tcp, allow,69059,10492,58567,78,2
016/11/15 08:44:24,59,govern ment,0,2816300982,0x0,US,US, 0,33,45,tcp-rst-from-client,
0,0,0,0,,ATL-PAN-01,from-pol icy
Nov 15 08:45:39 10.1.0.2 1,2016/11/15 08:45:39,00180 1015967,TRAFFIC,end,1,2016/1 1/15
08:45:39,64.85.77.9,50. 232.155.145,64.85.77.9,10.25 0.0.10,inbound-web-browsing, ,,web-
browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15
08:45:39,28555,1,40262,80,4 0262,80,0x40001c,tcp,allow,5 809,2726,3083,22,2016/11/15
08:44:52,31,government,0,281 6300989,0x0,US,US,0,14,8,tcp -rst-from-client,0,0,0,0,,AT L-
PAN-01,from-policy
Nov 15 08:45:39 10.1.0.2 1,2016/11/ 15 08:45:39,001801015967,TRA FFIC,end,1,2016/11/15
08:45: 39,64.85.77.2,50.232.155.145 ,64.85.77.2,10.250.0.10,inbo und-web-browsing,,,web-
brows ing,vsys1,outside,dmz,ethern et1/4,ethernet1/2,dell-secur eworks,2016/11/15 08:45:39,7

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

097,1,59652,80,59652,80,0x40 001c,tcp,allow,37219,7435,29 784,47,2016/11/15 08:44:23,6
0,government,0,2816301002,0x 0,US,US,0,24,23,tcp-fin,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:45:39 10.1.0.2 1,2 016/11/15 08:45:39,001801015 967,TRAFFIC,start,1,2016/11/ 15
08:45:39,66.192.63.2,50.2 32.155.145,66.192.63.2,10.25 0.0.10,inbound-web-browsing, ,,web-
browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15
08:45:39,42068,1,23777,80,2 3777,80,0x400000,tcp,allow,1 523,1449,74,4,2016/11/15 08:
45:39,0,any,0,2816301060,0x0 ,US,US,0,3,1,n/a,0,0,0,0,,AT L-PAN-01,from-policy
Nov 15 08:45:38 10.1.0.2 1,2016/11/ 15 08:45:38,001801015967,TRA
FFIC,start,1,2016/11/15 08:4 5:38,104.129.204.75,50.232.1
55.145,104.129.204.75,10.250 .0.10,inbound-web-browsing,, ,web-
browsing,vsys1,outside, dmz,ethernet1/4,ethernet1/2, dell-secureworks,2016/11/15
08:45:38,28484,1,2107,80,210 7,80,0x400000,tcp,allow,1299 ,1225,74,4,2016/11/15 08:45:
38,0,any,0,2816300963,0x0,US ,US,0,3,1,n/a,0,0,0,0,,ATL-P AN-01,from-policy
Nov 15 08: 45:38 10.1.0.2 1,2016/11/15 08:45:38,001801015967,TRAFFI C,end,1,2016/11/15
08:45:38, 12.167.43.50,50.232.155.145, 12.167.43.50,10.250.0.10,inb ound-web-
browsing,,,web-brow sing,vsys1,outside,dmz,ether net1/4,ethernet1/2,dell-secu
reworks,2016/11/15 08:45:38, 37849,1,52645,80,52645,80,0x 40001c,tcp,allow,31419,1888,
29531,42,2016/11/15 08:45:21 ,1,government,0,2816300902,0 x0,US,US,0,20,22,tcp-
fin,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:45:38 10.1.0.2 1, 2016/11/15 08:45:38,00180101 5967,TRAFFIC,end,1,2016/11/1
5 08:45:38,12.167.43.50,50.2 32.155.145,12.167.43.50,10.2 50.0.10,inbound-
web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-
secureworks,2016/11/1 5 08:45:38,38095,1,52646,80, 52646,80,0x40001c,tcp,allow,
8617,1205,7412,17,2016/11/15 08:45:21,1,government,0,281 6300862,0x0,US,US,0,10,7,tcp -
fin,0,0,0,0,,ATL-PAN-01,fro m-policy
Nov 15 08:45:38 10. 1.0.2 1,2016/11/15 08:45:38, 001801015967,TRAFFIC,end,1,2
016/11/15 08:45:38,12.167.43 .50,50.232.155.145,12.167.43 .50,10.250.0.10,inbound-web-
browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2
016/11/15 08:45:38,25542,1,5 2647,80,52647,80,0x40001c,tc p,allow,15931,1534,14397,27,
2016/11/15 08:45:22,0,govern ment,0,2816300860,0x0,US,US, 0,15,12,tcp-fin,0,0,0,0,,ATL -
PAN-01,from-policy
Nov 15 0 8:45:37 10.1.0.2 1,2016/11/1 5 08:45:37,001801015967,TRAF FIC,end,1,2016/11/15
08:45:3 7,12.167.43.50,50.232.155.14 5,12.167.43.50,10.250.0.10,i nbound-web-
browsing,,,web-br owsing,vsys1,outside,dmz,eth ernet1/4,ethernet1/2,dell-se

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

cureworks,2016/11/15 08:45:3 7,29246,1,52643,80,52643,80, 0x40001c,tcp,allow,1562,963,
599,9,2016/11/15 08:45:21,0, government,0,2816300728,0x0, US,US,0,6,3,tcp-
fin,0,0,0,0, ,ATL-PAN-01,from-policy
Nov 15 08:45:37 10.1.0.2 1,2016/ 11/15 08:45:37,001801015967, TRAFFIC,end,1,2016/11/15
08: 45:37,12.167.43.50,50.232.15 5.145,12.167.43.50,10.250.0. 10,inbound-web-browsing,,,we
b-browsing,vsys1,outside,dmz ,ethernet1/4,ethernet1/2,del l-secureworks,2016/11/15 08:
45:37,55425,1,52644,80,52644 ,80,0x40001c,tcp,allow,2472, 861,1611,9,2016/11/15 08:45:
21,0,government,0,2816300745 ,0x0,US,US,0,6,3,tcp-fin,0,0 ,0,0,,ATL-PAN-01,from-policy
Nov 15 08:45:37 10.1.0.2 1, 2016/11/15 08:45:37,00180101 5967,TRAFFIC,end,1,2016/11/1
5 08:45:37,12.167.43.50,50.2 32.155.145,12.167.43.50,10.2 50.0.10,inbound-
web-browsing ,,,web-browsing,vsys1,outsid e,dmz,ethernet1/4,ethernet1/ 2,dell-
secureworks,2016/11/1 5 08:45:37,11178,1,52642,80, 52642,80,0x40001c,tcp,allow,
1489,953,536,9,2016/11/15 08 :45:21,0,government,0,281630 0679,0x0,US,US,0,6,3,tcp-
fin ,0,0,0,0,,ATL-PAN-01,from-po licy
Nov 15 08:45:35 10.1.0. 2 1,2016/11/15 08:45:35,0018 01015967,TRAFFIC,start,1,201
6/11/15 08:45:35,108.66.253. 68,50.232.155.145,108.66.253 .68,10.250.0.10,inbound-web-
browsing,,,web-browsing,vsys 1,outside,dmz,ethernet1/4,et hernet1/2,dell-secureworks,2
016/11/15 08:45:35,42763,1,6 0738,80,60738,80,0x400000,tc p,allow,779,713,66,4,2016/11 /15
08:45:35,0,any,0,2816300 501,0x0,US,US,0,3,1,n/a,0,0, 0,0,,ATL-PAN-01,from-policy
Nov 15 08:45:36 10.1.0.2 1,2 016/11/15 08:45:36,001801015 967,TRAFFIC,end,1,2016/11/15
08:45:36,64.85.97.251,50.23 2.155.145,64.85.97.251,10.25 0.0.10,inbound-
web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-
secureworks,2016/11/15 08:45:36,29613,1,48440,80,4 8440,80,0x40001c,tcp,allow,4
4231,9690,34541,65,2016/11/1 5 08:45:15,5,government,0,28 16300538,0x0,US,US,0,37,28,t
cp-rst-from-client,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:45:36 10.1.0.2 1,2016/1 1/15 08:45:36,001801015967,T RAFFIC,end,1,2016/11/15
08:4 5:36,209.67.78.40,50.232.155 .145,209.67.78.40,10.250.0.1 0,inbound-
web-browsing,,,web -browsing,vsys1,outside,dmz, ethernet1/4,ethernet1/2,dell -
secureworks,2016/11/15 08:4 5:36,39848,1,52423,80,52423, 80,0x40001c,tcp,allow,4000,1
838,2162,15,2016/11/15 08:45 :17,3,government,0,281630053 7,0x0,US,US,0,10,5,tcp-
fin,0 ,0,0,0,,ATL-PAN-01,from-poli cy
Nov 15 08:45:35 10.1.0.2 1,2016/11/15 08:45:35,001801 015967,TRAFFIC,start,1,2016/
11/15 08:45:35,50.246.9.145, 50.232.155.145,50.246.9.145, 10.250.0.10,inbound-web-brow
sing,,,web-browsing,vsys1,ou tside,dmz,ethernet1/4,ethern et1/2,dell-secureworks,2016/

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

11/15 08:45:35,39115,1,28465 ,80,28465,80,0x400000,tcp,al low,1522,1456,66,4,2016/11/1 5 08:45:35,0,any,0,281630050 3,0x0,US,US,0,3,1,n/a,0,0,0, 0,,ATL-PAN-01,from-policy
No v 15 08:45:35 10.1.0.2 1,201 6/11/15 08:45:35,00180101596 7,TRAFFIC,end,1,2016/11/15 0 8:45:35,152.133.7.129,50.232 .155.145,152.133.7.129,10.25 0.0.10,inbound-web-browsing, ,,web-browsing,vsys1,outside ,dmz,ethernet1/4,ethernet1/2 ,dell-secureworks,2016/11/15 08:45:35,28206,1,47295,80,4 7295,80,0x40001a,tcp,allow,1 7045,5711,11334,23,2016/11/1 5 08:45:13,6,government,0,28 16300399,0x0,US,US,0,12,11,t cp-rst-from-client,0,0,0,0,, ATL-PAN-01,from-policy
Nov 1 5 08:45:35 10.1.0.2 1,2016/1 1/15 08:45:35,001801015967,T RAFFIC,start,1,2016/11/15 08 :45:35,50.246.9.145,50.232.1 55.145,50.246.9.145,10.250.0 .10,inbound-web-browsing,,,w eb-browsing,vsys1,outside,dm z,ethernet1/4,ethernet1/2,de ll-secureworks,2016/11/15 08 :45:35,27811,1,59271,80,5927 1,80,0x400000,tcp,allow,1521 ,1455,66,4,2016/11/15 08:45: 35,0,any,0,2816300475,0x0,US ,US,0,3,1,n/a,0,0,0,0,,ATL-P AN-01,from-policy
Nov 15 08: 45:34 10.1.0.2 1,2016/11/15 08:45:34,001801015967,TRAFFI C,end,1,2016/11/15 08:45:34, 64.85.77.7,50.232.155.145,64 .85.77.7,10.250.0.10,inbound -web-browsing,,,web-browsing ,vsys1,outside,dmz,ethernet1 /4,ethernet1/2,dell-securewo rks,2016/11/15 08:45:34,1494 7,1,53642,80,53642,80,0x4000 1c,tcp,allow,43265,9302,3396 3,58,2016/11/15 08:44:58,20, government,0,2816300288,0x0, US,US,0,30,28,tcp-fin,0,0,0, 0,,ATL-PAN-01,from-policy

15, Nov 2016 08:56:08 **automation** **Whois Information**

Whois Information
Source IP: 216.81.81.80

NetRange : 216.81.80.0 - 216.81 .95.255
CIDR: 216. 81.80.0/20
NetName: O NENET
NetHandle: NET-21 6-81-80-0-1
Parent: NET216 (NET-216-0-0-0-0)

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Net Type: Direct Assignme nt
OriginAS:
Organiza tion: DEPARTMENT OF HOMELA ND SECURITY (DHS-37)
RegDate : 2008-05-07
Updated: 2012-03-02
Ref: https://whois.arin.ne t/rest/net/NET-216-81-80-0-1

OrgName: DEPARTMEN T OF HOMELAND SECURITY
OrgId : DHS-37
Address: Department of Homeland Security
Address: 30 0 7th St SW
City: Washington
StateProv: D C
PostalCode: 20024
Coun try: US
RegDate: 2005-12-05
Updated: 2015-02-02
Ref: https://whois.arin.net/rest /org/DHS-37

OrgTechHandle: (b)(6)
OrgTechName: (b)(6)
OrgTechPhone: +1 -202-447-(b)(6)
OrgTechEmail: (b)(6)
Or gTechRef: https://whois.a rin.net/rest/poc/(b)(6)

OrgAbuseHandle: DHSNO2-ARIN
OrgAbuseName: DHS-NOC
Org AbusePhone: +1-202-447-(b)(6)
OrgAbuseEmail: onenetNMT@ hq.dhs.gov
OrgAbuseRef: h ttps://whois.arin.net/rest/p oc/DHSNO2-ARIN

OrgNOCHandle : DHSNO2-ARIN

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

OrgNOCName: DHS-NOC
OrgNOCPhone: +1-202 -447(b)(6)
OrgNOCEmail: one netNMT@hq.dhs.gov
OrgNOCRef: https://whois.arin.net/r est/poc/DHSNO2-ARIN

OrgTech Handle: DHSNO2-ARIN
OrgTechN ame: DHS-NOC
OrgTechPhone: +1-202-447-(b)(6)
OrgTechEm ail: onenetNMT@hq.dhs.gov
O rgTechRef: https://whois. arin.net/rest/poc/DHSNO2-ARI N

Destina tion IP: 50.232.155.145

NetRange: 50.128.0.0 - 50.255.255.255
CIDR: 50.128.0.0/9
NetName: CCCH3-4
NetHandle: NET-50-128-0-0-1
Parent: NET50 (NET-50-0-0-0- 0)
NetType: Direct Al location
OriginAS: AS7 922
Organization: Comcast Cable Communications, LLC (C CS)
RegDate: 2010-10 -21
Updated: 2016-08- 31
Ref: https://w hois.arin.net/rest/net/NET-5 0-128-0-0-1

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

OrgName: Comcast Cable Communicati ons, LLC
OrgId: CCC S
Address: 1800 Bisho ps Gate Blvd
City: Mt Laurel
StateProv: N J
PostalCode: 08054
Coun try: US
RegDate: 2001-09-18
Updated: 2008-10-04
Ref: https://whois.arin.net/rest /org/CCCS

OrgAbuseHandle: NAPO-ARIN
OrgAbuseName: Ne twork Abuse and Policy Obser vance
OrgAbusePhone: +1-888 -565-4329
OrgAbuseEmail: a buse@comcast.net
OrgAbuseRef : https://whois.arin.net/ rest/poc/NAPO-ARIN

OrgTechH andle: IC161-ARIN
OrgTechNam e: Comcast Cable Communica tions Inc
OrgTechPhone: +1- 856-317-7200
OrgTechEmail: CNIPEO-Ip-registration@cabl e.comcast.com
OrgTechRef: https://whois.arin.net/rest /poc/IC161-ARIN

15, Nov 2016 08:55:16 **SOC Staff** **Client Note**

IP Information for Ticket IN 23389418

---------- ---------- ---------- ----------

IP information for Destinati on - 50.232.155.145:
======= ========== ========== ==========

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Address type: Pub lic

Network: 50.232.155.128 /25 Public Aded via ticket number 19345964

---- ---------- ---------- ---------- ----------
There is no Vul nerability scan data for 50. 232.155.145

---------- ---------- ---------- ---------- -

IP information for Source - 216.81.81.80:
========== ========== ========== ==========
========== =====

Address type: Public

---------- ---------- ---------- ----------

No other clients have seen activity f rom 216.81.81.80 in the past 7 days.

---------- ---------- ---------- ----------

Not found on a SecureWorks m onitored blacklist.

Relat ed Incidents based on IP Add resses:
========== ==========
========== ==========
==========
23227193 2016-11-01 14:43:47 Closed Inconclusive Si lverSky Scanning Activity (F
ormerly E-Security)

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Bid irectional History based on IP Addresses:
========== ========== ========== ========== ==========
32481 554 2016-11-15 11:25:44 2 50.232.155.145 216 .186.180.100 Not Blocked File Alert: Adobe Portable D ocument Format (PDF)
3248634 0 2016-11-15 12:34:23 1 152.133.6.4 50.23 2.155.145 Not Blocked HT TP OPTIONS Method
32490269 2016-11-15 13:18:49 1 50.232.155.145 170.218 .219.21 Not Blocked File Alert: Adobe Portable Docum ent Format (PDF)
32491072 2016-11-15 13:26:45 1 104.148.75.107 50.232.15 5.145 Blocked [I]: U RL Blocked: "www.8xbxb.com/"
32491446 20 16-11-15 13:29:44 3 5 0.232.155.145 74.174.56.6 Not Blocked File Ale rt: Adobe Portable Document Format (PDF)
32493075 2016 -11-15 13:43:25 1 216 .81.81.80 50.232.155.14 5 Not Blocked HTTP OPTIO NS Method

15, Nov 2016 08:54:59 **automation** **Client Notification**

Communication Message:
Send To: (b)(6) gov;
Subj ect: SecureWorks Ticket #IN2 3389418 | New Ticket - Auto Assigned to (b)(6)
everity: Medium | Department of Homeland Security Scanni ng Activity
Next Generation Portal: https://portal.secur eworks.com/portal/incidents/ IN23389418
Legacy Portal: ht tps://portal.secureworks.com /tickets/show/IN23389418

Lo cation: Secretary of State, Georgia
Ticket Summary: Depa rtment of Homeland Security Scanning Activity
Assigned T o: (b)(6)
Customer's I nternal Ticket #

The follow ing ticket will be automatic ally assigned to (b)(6) the first point of contac t in the escalation procedur e. Please, submit a ticket v ia the Portal if you would l ike the ticket to be handled differently during escalati on.

Incident Details:

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

==== ==========
Incide nt Overview
========== =========
The CTOC has recei ved an alert for 'HTTP OPTIO NS Method' from your Palo Al to FW device (10.1.0.2/firew all01) for traffic (Not Bloc ked) sourcing from port 6363 6/tcp of 216.81.81.80 (Arlin gton, USA) destined to port 80/tcp of 50.232.155.145 (Fe asterville Trevose, USA) tha t occurred on 2016-11-15 at 08:43:22. These alerts are indicative of possible vulne rability scanning activity s ourcing from the Department of Homeland Security IP addr ess 216.81.81.80.

If this n otification was triggered fr om scheduled and authorized scanning and you no longer w ish to be notified of Depart ment of Homeland Security vu lnerability scanning activit y, please reply to this tick et and we can adjust event s tream notifications for your company accordingly. Other wise, please verify that Dep artment of Homeland Security is an authorized vulnerabil ity scanning vendor for your company and determine wheth er the current scanning acti vity is legitimate.

We are escalating this incident to you via a medium priority t icket and no phone call per our default handling policy. If you would like us to han dle these incidents differen tly in the future (see below for handling options), or i f you have any further quest ions or concerns, please let us know either by correspon ding to us via this ticket a nd delegating the ticket bac k to the SOC, or by calling us at 877-838-7960.

1) Fu ll escalation for Department of Homeland Security Vulner ability Scanning activity (e xplicit notification via a h igh priority ticket and a ph one call)
2) Automatically r esolve Department of Homelan d Security Vulnerability Sca nning activity to the portal (no explicit notification b ut events will be available for reporting purposes in th e portal)

Sincerely,
Secur eWorks SOC
========== ========
Technical Details
= ==========

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

No Technical Details for this e vent.
========== ===
References
========== ==========
No References f or this event.
========== ==========
Event Details
= ==========
Rel ated Events:
Event ID: 3249 3075
Event Summary: HTTP OPT IONS Method
Occurrence Count : 1
Event Count: 1

Host and Connection Information
Sour ce IP: 216.81.81.80
Source P ort: 63636
Source IP Geoloca tion: Arlington, USA
Destina tion IP: 50.232.155.145
Dest ination Port: 80
Destination IP Geolocation: Feastervill e Trevose, USA
Connection Di rectionality: INTERNAL
Proto col: TCP

Device Information
Device IP: 10.1.0.2
Device Name: firewall01
Log Time: 2 016-11-15 at 08:43:22
Actio n: Not Blocked
Vendor Classi fication: THREAT,vulnerabili ty
Vendor Priority: informat ional
Threat Name: HTTP OPTI ONS Method

SCWX Event Proce ssing Information

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

Sherlock R ule ID (SLE): (b)(6)
Inspec tor Rule ID: (b)(6)
Inspecto r Event ID: (b)(6)
Agent ID : (b)(6)

Event Detail:
Nov 15 08:43:23 10.1.0.2 1,2016 /11/15
08:43:22,001801015967 ,THREAT,vulnerability,1,2016 /11/15
08:43:22,216.81.81.80 ,50.232.155.145,216.81.81.80 ,10.250.0.10,inbound-
web-bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dell-
secureworks,2016 /11/15 08:43:22,247985,1,636 36,80,63636,80,0x402000,tcp,
alert,"",HTTP OPTIONS Method (30520),government,informati onal,client-to-server,500430
600,0x0,US,US,0,,0,,,1,,,,,, ,,0,0,0,0,0,,ATL-PAN-01,

[O :SECURITY]

ASCII Packet(s) :
[no entry]

Hex Packet(s):
[no entry]

SecureWorks Sec urity Analysis Team
877-838- 7960
https://portal.securewo rks.com

15, Nov 2016 08:54:58 **automation** **Escalation Note**

Escalation Notes were change d on 01/08/2016 01:51:29 PM
SUMMARY OF THOSE CHANGES:
A dded 'Possible PHP-CGI Strin g Parsing Vulnerability Expl oit Attempts - Ticket Only'

Obtained via FOIA by Judicial Watch, Inc.

Title	Ticket Detail Report
Subtitle	This page displays a list of tickets which match your search criteria.
Location	Secretary of State, Georgia

Ticket Detail

ESCALATION NOTES:
Locale
========== ==========
+ L ocation: <ST>,<COUNTRY>
+ Lo cal Time: <STZ> GMT -0000 / <DTZ> GMT -0000
+ Business H ours: Mon-Fri, 9AM-6PM

Mo difications to Actions/Sever ities:
========== ========== ===

--> Possible PHP-CGI St ring Parsing Vulnerability E xploit Attempts - Ticket Onl y Please! <--

+ Aside from the above: please follow Sec ureWorks Default Handling Po licy

Contact Order
====== ========== ==========

Ticket Handling
========== ========== ======

Special Handling I nstructions
========== ========== ========

External Ticket

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) R>
To:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Sean.mcafee>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) >"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Robert.karas>"
CC:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) s>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Kirk.Easton>"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Socdhsonenet.cbp.dhs.gov3a5>"; "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"
Subject:	FW: Scanning Activity originating from DHS IP address space (216.81.80.0/20) -> (204.250.12.0/24)
Date:	2016/12/09 15:28:36
Priority:	Normal
Type:	Note

Thank you for taking my call, (b)(6). It was great to connect again!

I'm afraid we may not have appropriately communicated our findings regarding the Princess Cruise event from last week. My team sent their findings to US-CERT, which may not have been correct (see below). If you'd like us to continue investigating, we'll need more information from Princess Cruise.

Given the speculation correlating the Princess Cruise event with the Georgia's, I want to ensure that our findings make it to the correct hands. We are clear that they are not related or malicious.

FYI - (b)(6) is no longer with the ESOC. (b)(6) is the Acting ESOC Chief. Please reach out to (b)(6) or (b)(6) the ESOC Operations Manager if you have any questions about these incidents going forward.

Please give me a call if you have any questions.

Best,
Boyden

From: (b)(6)
Sent: Monday, December 5, 2016 3:34 PM
To: US-CERT operation center <soc@us-cert.gov>
Cc: Rohner (b)(6) HQ.DHS.GOV> (b)(6) <(b)(6) hs.gov>; Easton, (b)(6) >; (b)(6)
Subject: RE: Scanning Activity originating from DHS IP address space (216.81.80.0/20) -> (204.250.12.0/24)

Obtained via FOIA by Judicial Watch, Inc.

Time	Device Ad	Source IP	Source Po	Destinatic	Destinatic	Request M	Status Cor	src_port	Device Ac	Request L	Request R	Request L	Bytes In	Bytes Out	Request C	Request F	Request C	Compone	Request U	Request U	Destination Geo Address
15 Nov 20	10.236.22!	10.243.15.	63636	50.232.15!	80	OPTIONS	200	56337	OBSERVEI	http://verify.sos.ga.	/verificati		260	233	Government/Legal		FLETC	Microsoft	verify.sos.	, United States	

sourcetype	bluecoat:proxysg:access:file
action	allowed
bytes	493
bytes_in	260
bytes_out	233
c_ip	10.243.15.188
c_port	56337
category	Government/Legal
cs_User_Agent	Microsoft Office Protocol Discovery
cs_bytes	233
cs_categories	Government/Legal
cs_host	verify.sos.ga.gov
cs_method	OPTIONS
cs_uri_path	/verification/stylesheets/
cs_uri_port	80
cs_uri_scheme	http
date	2016-11-15
dest	verify.sos.ga.gov
dest_host	verify.sos.ga.gov
duration	88
dvc	10.236.225.141
eventtype	bluecoat_proxy (proxy web)
	nix-all-logs
http_method	OPTIONS
http_user_agent	Microsoft Office Protocol Discovery
product	ProxySG
r_ip	50.232.155.145
rs_bytes	206
s_action	TCP_NC_MISS
s_cpu_util	27
s_hierarchy	FLETC
s_ip	10.236.225.141
s_source_port	63636
sc_bytes	260
sc_filter_result	OBSERVED
sc_status	200
sr_bytes	237
src	10.243.15.188
src_ip	10.236.225.141
src_port	56337
status	200
tag	proxy

Obtained via FOIA by Judicial Watch, Inc.

Time	Device Address	Source IP	Source Port	Destination IP
03 Oct 2016 11:41:32 EDT	10.76.225.142	10.101.194.178	10141	50.232.155.157

Obtained via FOIA by Judicial Watch, Inc.

Destination Port	Request Method	Status Code	Device Action
80	OPTIONS	403	DENIED

Obtained via FOIA by Judicial Watch, Inc.

Request URL	Request Referrer	Request URL File Name	Bytes In
http://www.sos.state.ga.us/corporations/		/corporations/	1329

Obtained via FOIA by Judicial Watch, Inc.

Bytes Out	Request Domain Category	Request File Type	Request Query	Component
204	Government/Legal	text/html;%20charset=UTF-8		ICE-CIS

Obtained via FOIA by Judicial Watch, Inc.

Request User Agent	Request URL Host	Destination Geo Address
Microsoft Office Protocol Discovery	www.sos.state.ga.us	, United States

Obtained via FOIA by Judicial Watch, Inc.

Time	Device Address	Source IP	Source Port	Destination IP
07 Nov 2016 13:15:43 EDT	10.76.225.146	10.56.189.65	52514	50.232.155.157

Obtained via FOIA by Judicial Watch, Inc.

Destination Port	Request Method	Status Code	Device Action
80	OPTIONS	403	DENIED

Obtained via FOIA by Judicial Watch, Inc.

Request URL	Request Referrer	Request URL File Name	Bytes In
http://www.sos.georgia.gov/plb/cosmetology/		/plb/cosmetology/	1327

Obtained via FOIA by Judicial Watch, Inc.

Bytes Out	Request Domain Category	Request File Type	Request Query	Component
207	Government/Legal	text/html;%20charset=UTF-8		ICE-CIS

Obtained via FOIA by Judicial Watch, Inc.

Request User Agent	Request URL Host	Destination Geo Address
Microsoft Office Protocol Discovery	www.sos.georgia.gov	, United States

Obtained via FOIA by Judicial Watch, Inc.

Time	Device Address	Source IP	Source Port	Destination IP
08 Nov 2016 08:35:21 EDT	10.76.225.140	10.243.15.188	38084	50.232.155.145

Obtained via FOIA by Judicial Watch, Inc.

Destination Port	Request Method	Status Code	Device Action
80	OPTIONS	200	OBSERVED

Obtained via FOIA by Judicial Watch, Inc.

Request URL	Request Referrer	Request URL File Name	Bytes In
http://verify.sos.ga.gov/verification/stylesheets/		/verification/stylesheets/	260

Obtained via FOIA by Judicial Watch, Inc.

Bytes Out	Request Domain Category	Request File Type	Request Query	Component
233	Government/Legal			FLETC

Obtained via FOIA by Judicial Watch, Inc.

Request User Agent	Request URL Host	Destination Geo Address
Microsoft Office Protocol Discovery	verify.sos.ga.gov	, United States

Obtained via FOIA by Judicial Watch, Inc.

Time	Device Address	Source IP	Source Port	Destination IP	Destination Port
06 Oct 2016 11:14:16 EDT	10.236.225.141	10.32.82.42	10865	50.232.155.145	80

Obtained via FOIA by Judicial Watch, Inc.

Request Method	Status Code	Device Action	Request URL
OPTIONS	200	OBSERVED	http://verify.sos.ga.gov/verification/stylesheets/

Obtained via FOIA by Judicial Watch, Inc.

Request Referrer	Request URL File Name	Bytes In	Bytes Out	Request Domain Category
	/verification/stylesheets/	260	233	Government/Legal

Obtained via FOIA by Judicial Watch, Inc.

Request File Type	Request Query	Component	Request User Agent
		FEMA_DESKTOP	Microsoft Office Protocol Discovery

Obtained via FOIA by Judicial Watch, Inc.

Request URL Host	Destination Geo Address
verify.sos.ga.gov	, United States

Obtained via FOIA by Judicial Watch, Inc.

Time	Device Address	Source IP	Source Port	Destination IP
12 Sep 2016 12:52:32 EDT	10.236.225.145	10.61.22.222	59180	50.232.155.157

Obtained via FOIA by Judicial Watch, Inc.

Destination Port	Request Method	Status Code	Device Action	Request URL
80	OPTIONS	403	DENIED	http://www.sos.georgia.gov/

Obtained via FOIA by Judicial Watch, Inc.

Request Referrer	Request URL File Name	Bytes In	Bytes Out	Request Domain Category
	/	1327	191	Government/Legal

Obtained via FOIA by Judicial Watch, Inc.

Request File Type	Request Query	Component	Request User Agent
text/html;%20charset=UTF-8		ICE-CIS	Microsoft Office Protocol Discovery

Obtained via FOIA by Judicial Watch, Inc.

Request URL Host	Destination Geo Address
www.sos.georgia.gov	, United States

Obtained via FOIA by Judicial Watch, Inc.

Time	Device Address	Source IP	Source Port	Destination IP
28 Sep 2016 08:54:15 EDT	10.76.225.142	10.56.189.94	51165	50.232.155.157

Obtained via FOIA by Judicial Watch, Inc.

Destination Port	Request Method	Status Code	Device Action
80	OPTIONS	403	DENIED

Obtained via FOIA by Judicial Watch, Inc.

Request URL	Request Referrer	Request URL File Name	Bytes In
http://sos.ga.gov/index.php/licensing/plb/		/index.php/licensing/plb/	1327

Obtained via FOIA by Judicial Watch, Inc.

Bytes Out	Request Domain Category	Request File Type	Request Query	Component
197	Government/Legal			ICE-CIS

Obtained via FOIA by Judicial Watch, Inc.

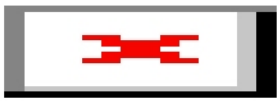
Request User Agent	Request URL Host	Destination Geo Address
Microsoft Office Protocol Discovery	sos.ga.gov	, United States

Obtained via FOIA by Judicial Watch, Inc.

From:	DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=SOCDHSONENET.CBP.DHS.GOV3A5>
SentVia:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
To:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) "
CC:	"/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Socdhsonenet.cbp.dhs.gov3a5>"
Subject:	Georgia Update
Date:	2016/12/09 13:02:36
Priority:	Normal
Type:	Note

Logs showing the traffic per our conversation.

v/r
(b)(6), GCIH, Sec+
Security Analyst, SOC – Shift Lead
General Dynamics Information Technology
Enterprise **S**ecurity **O**perations **C**enter (ESOC)
Department of Homeland Security
MGMT/OCIO/OCISO



dhs_esoc_2_info

Sender:	DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=SOCDHSONENET.CBP.DHS.GOV3A5>; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
Recipient:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) "; "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Socdhsonenet.cbp.dhs.gov3a5>"
Sent Date:	2016/12/09 13:02:34
Delivered Date:	2016/12/09 13:02:36

Obtained via FOIA by Judicial Watch, Inc.

Time	Device Address	Source IP	Source Po	Destination IP	Destinati	Request M	Device Action	Request URL	Request Referrer	Request U	Bytes In	Bytes Out	Request E	Request F	Request C	Compone	Request L	Request U	Destination Geo Address
15 Nov 2016 08:36:10 EDT	10.76.225.140	10.243.15.188	61784	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/images/banner.png	http://verify.sos.ga.gov/verification/	/verificati	13659	1853	Governm	image/png		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:36:10 EDT	10.76.225.140	10.243.15.188	61782	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/stylesheets/elicens	http://verify.sos.ga.gov/verification/	/verificati	343	1912	Governm	text/css		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:36:10 EDT	10.76.225.140	10.243.15.188	61778	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/images/menu_bac.jpg	http://verify.sos.ga.gov/verification/	/images/i	1467	1842	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:36:11 EDT	10.76.225.140	10.243.15.188	61699	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/		/verificati	28051	1774	Governm	text/html;%20charse		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:36:12 EDT	10.76.225.140	10.243.15.188	61699	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/Search.aspx?facilit	http://verify.sos.ga.gov/verification/	/verificati	24125	1845	Governm	text/html	?facility=\	FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:36:12 EDT	10.76.225.140	10.243.15.188	61784	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/images/menu_bac.jpg	http://verify.sos.ga.gov/verification/\	/images/i	1467	1864	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:36:19 EDT	10.76.225.140	10.243.15.188	61699	50.232.155.145	80	POST	OBSERVED	http://verify.sos.ga.gov/verification/Search.aspx?facilit	http://verify.sos.ga.gov/verification/\	/verificati	24406	6672	Governm	text/html	?facility=\	FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:36:23 EDT	10.76.225.140	10.243.15.188	61699	50.232.155.145	80	GET	DENIED	http://verify.sos.ga.gov/images/menu_bac.jpg	http://verify.sos.ga.gov/verification/\	/images/i	0	1891	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:36:23 EDT	10.76.225.140	10.243.15.188	61699	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/SearchResults.asp	http://verify.sos.ga.gov/verification/\	/verificati	5862	1881	Governm	text/html;%20charse		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:36:23 EDT	10.76.225.140	10.243.15.188	61699	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/Details.aspx?result=I	http://verify.sos.ga.gov/verification/\	/verificati	32185	1879	Governm	text/html	?result=B2	FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:36:23 EDT	10.76.225.140	10.243.15.188	61782	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/images/menu_bac.jpg	http://verify.sos.ga.gov/verification/D	/images/i	1467	1880	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:36:23 EDT	10.76.225.140	10.243.15.188	61784	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/javascript/function	http://verify.sos.ga.gov/verification/D	/verificati	1467	1880	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:42:55 EDT	10.76.225.140	10.243.15.188	38729	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/images/menu_bac.jpg	http://verify.sos.ga.gov/verification/D	/images/i	1467	1880	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:42:55 EDT	10.76.225.140	10.243.15.188	38740	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/javascript/function	http://verify.sos.ga.gov/verification/D	/verificati	1467	1880	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:42:55 EDT	10.76.225.140	10.243.15.188	38475	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/Details.aspx?result=I	http://verify.sos.ga.gov/verification/\	/verificati	32185	1879	Governm	text/html	?result=B2	FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 08:43:18 EDT	10.236.225.141	10.243.15.188	0	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/stylesheets/elicense2000.css		/verificati	343	475	Governm	text/css		FLETC	Mozilla/4.	verify.sos	, United States
15 Nov 2016 08:43:18 EDT	10.236.225.141	10.243.15.188	0	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/stylesheets/elicense2000.css		/verificati	343	475	Governm	text/css		FLETC	Mozilla/4.	verify.sos	, United States
15 Nov 2016 08:43:18 EDT	10.236.225.141	10.243.15.188	63636	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/stylesheets/elicense2000.css		/verificati	319	475	Governm	text/css		FLETC	Mozilla/4.	verify.sos	, United States
15 Nov 2016 08:43:18 EDT	10.236.225.141	10.243.15.188	63636	50.232.155.145	80	OPTIONS	OBSERVED	http://verify.sos.ga.gov/verification/stylesheets/		/verificati	260	233	Governm	text/Legal		FLETC	Microsoft	verify.sos	, United States
15 Nov 2016 16:01:21 EDT	10.76.225.140	10.243.15.188	61416	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/images/footer.png	http://verify.sos.ga.gov/verification/	/verificati	296	1937	Governm	image/png		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:21 EDT	10.76.225.140	10.243.15.188	61421	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/images/banner.png	http://verify.sos.ga.gov/verification/	/verificati	298	1939	Governm	image/png		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:21 EDT	10.76.225.140	10.243.15.188	61416	50.232.155.145	80	GET	DENIED	http://verify.sos.ga.gov/images/menu_bac.jpg	http://verify.sos.ga.gov/verification/	/images/i	0	1842	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:21 EDT	10.76.225.140	10.243.15.188	61396	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/stylesheets/elicens	http://verify.sos.ga.gov/verification/	/verificati	343	1912	Governm	text/css		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:21 EDT	10.76.225.140	10.243.15.188	61345	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/		/verificati	28051	1774	Governm	text/html;%20charse		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:22 EDT	10.76.225.140	10.243.15.188	61421	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/images/menu_bac.jpg	http://verify.sos.ga.gov/verification/\	/images/i	1467	1864	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:22 EDT	10.76.225.140	10.243.15.188	61416	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/Search.aspx?facilit	http://verify.sos.ga.gov/verification/	/verificati	24125	1845	Governm	text/html	?facility=\	FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:30 EDT	10.76.225.140	10.243.15.188	61421	50.232.155.145	80	POST	OBSERVED	http://verify.sos.ga.gov/verification/Search.aspx?facilit	http://verify.sos.ga.gov/verification/\	/verificati	24406	6672	Governm	text/html	?facility=\	FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:31 EDT	10.76.225.140	10.243.15.188	61421	50.232.155.145	80	GET	DENIED	http://verify.sos.ga.gov/images/menu_bac.jpg	http://verify.sos.ga.gov/verification/\	/images/i	0	1891	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:31 EDT	10.76.225.140	10.243.15.188	61421	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/SearchResults.asp	http://verify.sos.ga.gov/verification/\	/verificati	5862	1881	Governm	text/html;%20charse		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:34 EDT	10.76.225.140	10.243.15.188	61421	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/images/menu_bac.jpg	http://verify.sos.ga.gov/verification/D	/images/i	1467	1880	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:34 EDT	10.76.225.140	10.243.15.188	61416	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/javascript/function	http://verify.sos.ga.gov/verification/D	/verificati	1467	1880	Governm	text/htm		FLETC	Mozilla/5.	verify.sos	, United States
15 Nov 2016 16:01:34 EDT	10.76.225.140	10.243.15.188	61421	50.232.155.145	80	GET	OBSERVED	http://verify.sos.ga.gov/verification/Details.aspx?result=	http://verify.sos.ga.gov/verification/\	/verificati	32185	1879	Governm	text/html	?result=Dr	FLETC	Mozilla/5.	verify.sos	, United States

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>
To:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"
Subject:	Info for Georgia
Date:	2016/12/15 18:41:30
Priority:	Normal
Type:	Note.SMIME.MultipartSigned

Can you get me the links you were researching on OPTIONS? The MS one (I might already have that) and the RFC?

Thanks in advance.

(b)(6)
(Acting) Chief, DHS ESOC
Office of the Chief Information Security Officer
Department of Homeland Security
Mobile: 202-657-(b)(6)

Sender:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>
Recipient:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
Sent Date:	2016/12/15 18:41:29
Delivered Date:	2016/12/15 18:41:30

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
To:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; "(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6); '(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; '(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; '(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"
CC:	"DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Socdhsonenet.cbp.dhs.gov3a5>"; "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"
Subject:	Re: Afernoon GA Update
Date:	2016/12/16 17:01:30
Type:	Note

(b)(6)

Appreciate the good work here.

From: (b)(6)
Sent: Friday, December 16, 2016 04:27 PM
To: (b)(6)
(b)(6)
Cc: DHS ESOC; DHS ESOC Leads (b)(6)
Subject: Afernoon GA Update

Good evening,

Today's updates:

-(b)(6) and I briefed:
1) Congressional staffers and GA Congressman Laudermilk,
2) the National Association of Secretaries of State (NASS) - including Secretary Kemp
3) and the press.

-Initial reports from OPA and OLA are favorable. They will be monitoring press throughout the weekend.

Obtained via FOIA by Judicial Watch, Inc.

- OLA is sending a follow write-up to the Hill based on the briefing memo drafted yesterday.

-The NASS asked for a list of our 14 IPs for future reference. If it's ok with you, Jeff, we will send them.

-Although we received no additional information from GA's CIO, we agreed to send them our logs showing that DHS recreated the event, since none of our recreations have flagged and alert.

I'm not tracking other any other action items.

From: (b)(6)
Sent: Thursday, December 15, 2016 9:00:42 PM
To: (b)(6)
(b)(6)
Cc: DHS ESOC; DHS ESOC Leads; (b)(6)
Subject: Afernoon GA Update

Good evening,

Today's updates:

-The ESOC and Component SOCs have completed our search of all available DHS logs and the firewall logs that GA sent on Monday. We have no new information to report.

-We have not heard back from the GA CIO since we requested additional information from him yesterday. We left a voice message and emailed him today.

(b)(6) is waiting for a response from Microsoft regarding their level of public support.

-We are waiting to hear if we will brief the Hill.

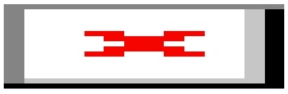
-The draft briefing memo for the Hill brief is attached for comments.

Barring any developments, the ESOC will send out another update at 4 pm tomorrow.

Best,

(b)(6)
Director, Cybersecurity Operations
MGMT/CIO/CISO
O: (202) 372-(b)(6)
M: (202) 657

Obtained via FOIA by Judicial Watch, Inc.



cid:image002.png@01D15F3C.8E63B2B0

Sender:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>
Recipient:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Socdhsonenet.cbp.dhs.gov3a5>"; "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"
Sent Date:	2016/12/16 17:01:29
Delivered Date:	2016/12/16 17:01:30

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
To:	"(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"
Subject:	RE: Details on the Georgia SoS Event
Date:	2016/12/09 12:45:03
Priority:	Normal
Type:	Note

ESOC acknowledges. We will start running this down. Thanks,(b)(6)

Best,

Obtained via FOIA by Judicial Watch, Inc.

(b)(6)

DHS Enterprise Security Operations Center (ESOC)
MGMT/OCIO/CISO/SOC
Supporting the Department of Homeland Security (DHS)
General Dynamics Information Technology

Direct Work: (540) 542(b)(6)
BlackBerry: (202)-309-

Great leaders have a heart for people.
They take time for people.
They view people as the bottom line,
Not as a tool to get to the bottom line.

From: (b)(6) (CTR)
Sent: Friday, December 9, 2016 12:43 PM
To: (b)(6)
(b)(6)
(b)(6)
u,
(b)(6)
Subject: FW: Details on the Georgia SoS Event

See below –K

From: (b)(6)
Sent: Friday, December 9, 2016 12:40 PM
To: DHS ESOC Leads <DHSESOCLeads@hq.dhs.gov>
Subject: Details on the Georgia SoS Event

ALCON –

Obtained via FOIA by Judicial Watch, Inc.

Just got off the phone with the CIO for the Georgia SoS. He was very helpful and was able to provide the following details regarding the potential scan event:

Source IP:
216.81.81.80:63636

Destination IP:
52.232.155.145:80

Start Time
0743 CST

Number of Events:
1 in an 8 hour window.

Scan Type:
HTTP Options

Please investigate this and provide results ASAP.

Thanks in advance and let me know if you have any questions.

(b)(6)
(Acting) Chief, DHS ESOC
Office of the Chief Information Security Officer
Department of Homeland Security
Mobile: 202-657-(b)(6)

Sender:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=GRANT.PEREGOY.DHSHQ.DHS.GOVA40>
Recipient:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Rommel.cordoba.associates.hq.dhs.govd2c>"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; '(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6); (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)

Obtained via FOIA by Judicial Watch, Inc.

	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6); (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)'; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)'; (b)(6) CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; "(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)'; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6); (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)'; (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6); (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"
Sent Date:	2016/12/09 12:45:02
Delivered Date:	2016/12/09 12:45:03

Obtained via FOIA by Judicial Watch, Inc.

Time	Device Address	Source IP	Source Port	Destination IP	Destination Port	Request Method	Device Action	Request URL	Request Referrer	Request URL File Name	Bytes In	Bytes Out	Request Protocol	Request Protocol Version	Request Client Application	Request User Agent	Request URL Host	Destination Geo Address
15 Nov 2016 00:21:39 EST	10.76.225.140	10.243.15.188	61822	23.101.30.126	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	4551	925	Office/Business Applications	FIETC			nexus.officeapp	, Singapore
15 Nov 2016 00:21:39 EST	10.76.225.140	10.243.15.188	61969	104.46.38.64	443	CONNECT	OBSERVED	http://nexusrules.officeapps.live.com/		/	4199	940	Office/Business Applications	FIETC			nexusrules.offe	Redmond, United States
15 Nov 2016 01:04:09 EST	10.76.225.140	10.243.15.188	36731	40.84.192.103	443	CONNECT	OBSERVED	http://odc.officeapps.live.com/		/	4769	775	Technology/Internet	FIETC			odc.officeapps.l	San Antonio, United States
15 Nov 2016 01:07:38 EST	10.76.225.140	10.243.15.188	47560	191.237.218.231	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	4551	925	Office/Business Applications	FIETC			nexus.officeapp	, United States
15 Nov 2016 01:07:38 EST	10.76.225.140	10.243.15.188	47603	104.46.38.64	443	CONNECT	OBSERVED	http://nexusrules.officeapps.live.com/		/	4199	940	Office/Business Applications	FIETC			nexusrules.offe	Redmond, United States
15 Nov 2016 01:53:38 EST	10.236.225.141	10.243.15.188	25168	65.52.28.28	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	4551	925	Office/Business Applications	FIETC			nexus.officeapp	Redmond, United States
15 Nov 2016 01:53:38 EST	10.236.225.141	10.243.15.188	25178	23.99.108.44	443	CONNECT	OBSERVED	http://nexusrules.officeapps.live.com/		/	4199	940	Office/Business Applications	FIETC			nexusrules.offe	Hong Kong, Hong Kong
15 Nov 2016 02:39:38 EST	10.236.225.141	10.243.15.188	23449	23.100.88.93	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	4551	925	Office/Business Applications	FIETC			nexus.officeapp	Des Moines, United States
15 Nov 2016 02:39:38 EST	10.236.225.141	10.243.15.188	23491	40.113.8.255	443	CONNECT	OBSERVED	http://nexusrules.officeapps.live.com/		/	4199	940	Office/Business Applications	FIETC			nexusrules.offe	Dublin, Ireland
15 Nov 2016 02:47:04 EST	10.76.225.140	10.243.15.188	0	199.167.93.70	80	GET	OBSERVED	http://http.fpki.gov/fcpca/fcpca.crl		/fcpca/fcpca.crl	1136	154	Governm	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	http.fpki.gov	Fairfax, United States
15 Nov 2016 02:47:35 EST	10.76.225.140	10.243.15.188	0	166.123.219.26	80	GET	OBSERVED	http://pki.treasury.gov/US_Treasury_Root_CA.crl		/pki_Treasury_Root_CA.crl	322	286	Governm	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	pki.treasury.gov	Washington, United States
15 Nov 2016 02:47:35 EST	10.76.225.140	10.243.15.188	0	184.26.143.114	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/MicrosoftTimeStampPCA.crl		/pki/crl/products/MicrosoftTimeStampPCA.crl	482	305	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 02:47:35 EST	10.76.225.140	10.243.15.188	0	184.26.143.114	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/CodeSignPCA.crl		/pki/crl/products/CodeSignPCA.crl	481	294	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 02:47:35 EST	10.76.225.140	10.243.15.188	0	23.208.179.27	80	GET	OBSERVED	http://www.microsoft.com/pki/crl/products/WinPCA.crl		/pki/crl/products/WinPCA.crl	547	289	Technolo	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	www.microsoft.c	Amsterdam, Netherlands
15 Nov 2016 02:47:35 EST	10.76.225.140	10.243.15.188	0	23.208.179.27	80	GET	OBSERVED	http://www.microsoft.com/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl		/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl	548	304	Technolo	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	www.microsoft.c	Amsterdam, Netherlands
15 Nov 2016 02:47:35 EST	10.76.225.140	10.243.15.188	0	184.26.143.114	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl		/pki/crl/products/CodeSignPCA2.crl	481	295	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 02:47:35 EST	10.76.225.140	10.243.15.188	0	184.26.143.114	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/MicCodSigPCA_08-31-2010.crl		/pki/crl/products/MicCodSigPCA_08-31-2010.crl	481	306	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 02:47:35 EST	10.76.225.140	10.243.15.188	0	184.26.143.114	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl		/pki/crl/products/microsoftrootcert.crl	479	298	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 02:47:35 EST	10.76.225.140	10.243.15.188	0	184.26.143.114	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl		/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	482	311	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 02:47:35 EST	10.76.225.140	10.243.15.188	0	184.26.143.114	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/tspca.crl		/pki/crl/products/tspca.crl	478	288	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 02:47:35 EST	10.76.225.140	10.243.15.188	0	23.208.179.27	80	GET	OBSERVED	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl		/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	547	303	Technolo	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	www.microsoft.c	Amsterdam, Netherlands
15 Nov 2016 03:01:37 EST	10.236.225.141	10.243.15.188	8880	72.21.81.200	443	CONNECT	OBSERVED	http://r20swj13mr.microsoft.com/		/r20swj13mr.microsoft.com/	7015	1564	Technology/Internet	FIETC	Mozilla/5.0 (Windows NT 6.1; Win64; x64)	r20swj13mr.mic	Santa Monica, United States
15 Nov 2016 03:01:37 EST	10.236.225.141	10.243.15.188	8879	72.21.81.200	443	CONNECT	OBSERVED	http://ocsi.ctl.microsoft.com/		/	6866	1407	Technology/Internet	FIETC			ocsi.ctl.microso	Seattle, United States
15 Nov 2016 03:25:39 EST	10.76.225.140	10.243.15.188	24532	23.99.116.116	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	4551	925	Office/Business Applications	FIETC			nexus.officeapp	Hong Kong, Hong Kong
15 Nov 2016 03:25:39 EST	10.76.225.140	10.243.15.188	24533	104.46.38.64	443	CONNECT	OBSERVED	http://nexusrules.officeapps.live.com/		/	4199	940	Office/Business Applications	FIETC			nexusrules.offe	Hong Kong, Hong Kong
15 Nov 2016 04:11:38 EST	10.236.225.141	10.243.15.188	18949	104.210.40.87	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	4551	925	Office/Business Applications	FIETC			nexus.officeapp	Redmond, United States
15 Nov 2016 04:11:38 EST	10.236.225.141	10.243.15.188	18967	40.113.8.255	443	CONNECT	OBSERVED	http://nexusrules.officeapps.live.com/		/	4199	940	Office/Business Applications	FIETC			nexusrules.offe	Dublin, Ireland
15 Nov 2016 04:42:21 EST	10.76.225.140	10.243.15.188	18251	40.84.192.103	443	CONNECT	OBSERVED	http://odc.officeapps.live.com/		/	4769	775	Technology/Internet	FIETC			odc.officeapps.l	San Antonio, United States
15 Nov 2016 04:57:39 EST	10.76.225.140	10.243.15.188	61585	23.102.155.140	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	4551	925	Office/Business Applications	FIETC			nexus.officeapp	Redmond, United States
15 Nov 2016 04:57:39 EST	10.76.225.140	10.243.15.188	61610	13.76.219.230	443	CONNECT	OBSERVED	http://nexusrules.officeapps.live.com/		/	4199	940	Office/Business Applications	FIETC			nexusrules.offe	Singapore, Singapore
15 Nov 2016 05:49:39 EST	10.76.225.140	10.243.15.188	56161	104.46.50.125	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	4551	925	Office/Business Applications	FIETC			nexus.officeapp	Redmond, United States
15 Nov 2016 05:49:39 EST	10.76.225.140	10.243.15.188	56188	168.63.18.79	443	CONNECT	OBSERVED	http://nexusrules.officeapps.live.com/		/	4199	940	Office/Business Applications	FIETC			nexusrules.offe	, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	0	166.123.219.25	80	GET	OBSERVED	http://pki.treasury.gov/US_Treasury_Root_CA.crl		/US_Treasury_Root_CA.crl	321	286	Governm	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	pki.treasury.go	Washington, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	0	184.26.143.114	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/MicrosoftTimeStampPCA.crl		/pki/crl/products/MicrosoftTimeStampPCA.crl	482	305	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	0	184.26.143.129	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/CodeSignPCA.crl		/pki/crl/products/CodeSignPCA.crl	481	294	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	0	23.73.164.188	80	GET	OBSERVED	http://www.microsoft.com/pki/crl/products/WinPCA.crl		/pki/crl/products/WinPCA.crl	547	289	Technolo	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	www.microsoft.c	Amsterdam, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	0	23.73.164.188	80	GET	OBSERVED	http://www.microsoft.com/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl		/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl	548	304	Technolo	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	www.microsoft.c	Amsterdam, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	0	184.26.143.129	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl		/pki/crl/products/CodeSignPCA2.crl	481	295	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	0	184.26.143.129	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/MicCodSigPCA_08-31-2010.crl		/pki/crl/products/MicCodSigPCA_08-31-2010.crl	479	306	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	0	184.26.143.129	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl		/pki/crl/products/microsoftrootcert.crl	479	298	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	0	184.26.143.129	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl		/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	482	311	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	0	184.26.143.129	80	GET	OBSERVED	http://crl.microsoft.com/pki/crl/products/tspca.crl		/pki/crl/products/tspca.crl	478	288	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	0	23.73.164.188	80	GET	OBSERVED	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl		/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	547	303	Technolo	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	www.microsoft.c	Amsterdam, United States
15 Nov 2016 06:25:50 EST	10.76.225.140	10.243.15.188	6523	184.26.143.122	80	GET	OBSERVED	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?175ad		/msdownload/update/v3/static/trustedr/e	262	322	Non-Mic	application/vnd.ms-cab-compressed	FIETC	Microsoft-CryptoAPI/6.1	ctldl.windowsu	Cambridge, United States
15 Nov 2016 06:29:38 EST	10.236.225.141	10.243.15.188	55297	104.214.9.240	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	4551	925	Office/Business Applications	FIETC			nexus.officeapp	Redmond, United States
15 Nov 2016 06:29:38 EST	10.236.225.141	10.243.15.188	55320	168.63.129.17	443	CONNECT	OBSERVED	http://nexusrules.officeapps.live.com/		/	4199	940	Office/Business Applications	FIETC			nexusrules.offe	, United States
15 Nov 2016 07:15:39 EST	10.76.225.140	10.243.15.188	5663	104.45.11.195	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	4551	925	Office/Business Applications	FIETC			nexus.officeapp	Amsterdam, Netherlands
15 Nov 2016 07:15:39 EST	10.76.225.140	10.243.15.188	5783	168.63.18.79	443	CONNECT	OBSERVED	http://nexusrules.officeapps.live.com/		/	4199	940	Office/Business Applications	FIETC			nexusrules.offe	, United States
15 Nov 2016 07:47:09 EST	10.76.225.140	10.243.15.188	42400	40.76.62.115	443	CONNECT	OBSERVED	http://odc.officeapps.live.com/		/	4769	775	Technology/Internet	FIETC			odc.officeapps.l	Washington, United States
15 Nov 2016 07:47:15 EST	10.76.225.140	0		80	GET	DENIED		http://autodiscover.fletc.dhs.gov/autodiscover/autodiscover.xml		/autodiscover/autodiscover.xml	5463	450	Governm	text/xml	FIETC	Microsoft Office/15.0 (Windows NT 6.1	autodiscover.fletc.dhs.gov	
15 Nov 2016 07:47:15 EST	10.76.225.140	0		443	CONNECT	DENIED		http://autodiscover.fletc.dhs.gov/		/	185	63	Governm	text/html	FIETC		autodiscover.fletc.dhs.gov	
15 Nov 2016 07:47:15 EST	10.76.225.140	0		443	CONNECT	DENIED		http://fletc.dhs.gov/		/	185	63	Governm	text/html	FIETC		fletc.dhs.gov	
15 Nov 2016 07:47:21 EST	10.76.225.140	0	184.26.143.129	80	GET	OBSERVED		http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl		/pki/crl/products/MicRooCerAut2011_2011_	482	311	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 07:47:21 EST	10.76.225.140	0	184.26.143.129	80	GET	OBSERVED		http://crl.microsoft.com/pki/crl/products/tspca.crl		/pki/crl/products/tspca.crl	478	288	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 07:47:21 EST	10.76.225.140	0	23.208.179.27	80	GET	OBSERVED		http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl		/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	547	303	Technolo	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	www.microsoft.c	Amsterdam, Netherlands
15 Nov 2016 07:47:22 EST	10.76.225.140	0	166.123.219.25	80	GET	OBSERVED		http://pki.treasury.gov/US_Treasury_Root_CA.crl		/US_Treasury_Root_CA.crl	322	286	Governm	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	pki.treasury.go	Washington, United States
15 Nov 2016 07:47:22 EST	10.76.225.140	0	184.26.143.129	80	GET	OBSERVED		http://crl.microsoft.com/pki/crl/products/MicrosoftTimeStampPCA.crl		/pki/crl/products/MicrosoftTimeStampPCA.crl	482	305	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 07:47:22 EST	10.76.225.140	0	184.26.143.129	80	GET	OBSERVED		http://crl.microsoft.com/pki/crl/products/CodeSignPCA.crl		/pki/crl/products/CodeSignPCA.crl	481	294	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 07:47:22 EST	10.76.225.140	0	23.208.179.27	80	GET	OBSERVED		http://www.microsoft.com/pki/crl/products/WinPCA.crl		/pki/crl/products/WinPCA.crl	547	289	Technolo	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	www.microsoft.c	Amsterdam, Netherlands
15 Nov 2016 07:47:22 EST	10.76.225.140	0	23.208.179.27	80	GET	OBSERVED		http://www.microsoft.com/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl		/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl	548	304	Technolo	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	www.microsoft.c	Amsterdam, Netherlands
15 Nov 2016 07:47:22 EST	10.76.225.140	0	184.26.143.129	80	GET	OBSERVED		http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl		/pki/crl/products/CodeSignPCA2.crl	481	295	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 07:47:22 EST	10.76.225.140	0	184.26.143.129	80	GET	OBSERVED		http://crl.microsoft.com/pki/crl/products/MicCodSigPCA_08-31-2010.crl		/pki/crl/products/MicCodSigPCA_08-31-2010.crl	479	306	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 07:47:22 EST	10.76.225.140	0	184.26.143.129	80	GET	OBSERVED		http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl		/pki/crl/products/microsoftrootcert.crl	479	298	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 07:47:22 EST	10.76.225.140	0	184.26.143.129	80	GET	OBSERVED		http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl		/pki/crl/products/MicRooCerAut2011_2011_	482	311	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 07:47:22 EST	10.76.225.140	0	184.26.143.129	80	GET	OBSERVED		http://crl.microsoft.com/pki/crl/products/tspca.crl		/pki/crl/products/tspca.crl	478	288	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 07:47:22 EST	10.76.225.140	0	23.208.179.27	80	GET	OBSERVED		http://www.microsoft.com/pki/crl/products/WinPCA.crl		/pki/crl/products/WinPCA.crl	547	289	Technolo	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	www.microsoft.c	Amsterdam, Netherlands
15 Nov 2016 07:47:22 EST	10.76.225.140	0	23.208.179.27	80	GET	OBSERVED		http://www.microsoft.com/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl		/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl	548	304	Technolo	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	www.microsoft.c	Amsterdam, Netherlands
15 Nov 2016 07:47:22 EST	10.76.225.140	0	184.26.143.129	80	GET	OBSERVED		http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl		/pki/crl/products/CodeSignPCA2.crl	481	295	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 07:47:22 EST	10.76.225.140	0	184.26.143.129	80	GET	OBSERVED		http://crl.microsoft.com/pki/crl/products/MicCodSigPCA_08-31-2010.crl		/pki/crl/products/MicCodSigPCA_08-31-2010.crl	479	306	Non-Mic	application/pkix-crl	FIETC	Microsoft-CryptoAPI/6.1	crl.microsoft.co	Cambridge, United States
15 Nov 2016 07:48:16 EST	10.76.225.140	10.243.15.188	54697	23.96.95.202	443	CONNECT	OBSERVED	http://store.office.com/		/	7052	1095	Technology/Internet	FIETC			store.office.com	Washington, United States
15 Nov 2016 07:48:17 EST	10.76.225.140	10.243.15.188	54648	23.96.95.202	443	CONNECT	OBSERVED	http://store.office.com/		/	6984	962	Technology/Internet	FIETC			store.office.com	Washington, United States
15 Nov 2016 07:48:17 EST	10.76.225.140	10.243.15.188	54156	65.52.233.207	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	4567	925	Office/Business Applications	FIETC			nexus.officeapp	Redmond, United States
15 Nov 2016 07:48:17 EST	10.76.225.140	10.243.15.188	54649	23.96.95.202	443	CONNECT	OBSERVED	http://store.office.com/		/	10189	1697	Technology/Internet	FIETC			store.office.com	Washington, United States
15 Nov 2016 07:48:17 EST	10.76.225.140	10.243.15.188	54650	40.76.62.115	443	CONNECT	OBSERVED	http://odc.officeapps.live.com/		/	4769	775	Technology/Internet	FIETC			odc.officeapps.l	Washington, United States
15 Nov 2016 07:48:17 EST	10.76.225.140	10.243.15.188	54338	13.76.218.117	443	CONNECT	OBSERVED	http://nexusrules.officeapps.live.com/		/	9255	940	Office/Business Applications	FIETC			nexusrules.offe	Singapore, Singapore
15 Nov 2016 07:49:13 EST	10.76.225.140	10.243.15.188	54821	137.135.9.112	443	CONNECT	OBSERVED	http://wikipedia.firstpartyapps.oaspapps.com/		/	4718	2465	Office/Business Applications	FIETC	Mozilla/4.0 (compatible; MSIE 7.0; Win	wikipedia.firstp	, United States
15 Nov 2016 07:52:05 EST	10.76.225.140	10.243.15.188	38682	52.84.26.13	80	GET	OBSERVED	http://jwpsrv.com/library/DgdotHpeEeSi8woORWfmyA.js	http://dhsconnect.dhs.gov/pages/default.aspx	/library/DgdotHpeEeSi8woORWfmyA.js	27127	360	Content-T	text/javascript	FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	jwpsrv.com	Seattle, United States
15 Nov 2016 07:52:07 EST	10.76.225.140	0		216.58.229.206	443	CONNECT	DENIED			/	175	238	Web Ads/Analytics		FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	www.google-an	Mountain View, United States
15 Nov 2016 07:52:08 EST	10.76.225.140	0		162.247.242.18	443	CONNECT	DENIED			/	175	220	Web Ads/Analytics		FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	ssarc-nr-data.ne	, United States
15 Nov 2016 07:52:09 EST	10.76.225.140	10.243.15.188	30351	23.73.164.44	80	GET	OBSERVED	http://clients1.google.com/complete/search?hl=en-US&q=time&client=ie8&inputencoding=UTF-8&output=t	/complete/search	/complete/search	625	1622	Technolo	application/x-javascr	FIETC	Microsoft-CryptoAPI/6.1	clients1.google.	Mountain View, United States
15 Nov 2016 07:52:24 EST	10.76.225.140	0		216.58.229.238	443	CONNECT	DENIED			/	175	238	Web Ads/Analytics		FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	www.google-an	Mountain View, United States
15 Nov 2016 07:52:25 EST	10.76.225.140	0		162.247.242.18	443	CONNECT	DENIED			/	175	220	Web Ads/Analytics		FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	ssarc-nr-data.ne	, United States
15 Nov 2016 07:52:54 EST	10.243.15.188	41160	40.76.62.115	443	CONNECT	OBSERVED	http://odc.officeapps.live.com/		/	4769	775	Technology/Internet	FIETC			odc.officeapps.l	Washington, United States
15 Nov 2016 07:52:55 EST	10.236.225.141	3409	104.214.95.244	443	CONNECT	OBSERVED	http://nexus.officeapps.live.com/		/	5308	1804	Office/Business Applications	FIETC			nexus.officeapp	Redmond, United States
15 Nov 2016 07:53:08 EST	10.76.225.140	44636	40.76.62.115	443	CONNECT	OBSERVED	http://odc.officeapps.live.com/		/	4769	775	Technology/Internet	FIETC			odc.officeapps.l	Washington, United States
15 Nov 2016 07:54:13 EST	10.76.225.140	44034	23.78.164.55	443	CONNECT	OBSERVED	http://www.dhs.gov/		/	668	1183	Government/Legal	FIETC			www.dhs.gov	Cambridge, United States
15 Nov 2016 07:54:13 EST	10.76.225.140	44092	23.78.164.55	443	CONNECT	OBSERVED	http://www.dhs.gov/		/	11218	2294	Government/Legal	FIETC			www.dhs.gov	Cambridge, United States
15 Nov 2016 07:54:13 EST	10.76.225.140	39482	52.84.26.13	80	GET	OBSERVED	http://jwpsrv.com/library/DgdotHpeEeSi8woORWfmyA.js	http://dhsconnect.dhs.gov/pages/default.aspx	/library/DgdotHpeEeSi8woORWfmyA.js	27127	360	Content-T	text/javascript	FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	jwpsrv.com	Seattle, United States
15 Nov 2016 07:54:14 EST	10.76.225.140	0		162.247.242.18	443	CONNECT	DENIED			/	175	220	Web Ads/Analytics		FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	ssarc-nr-data.ne	, United States
15 Nov 2016 07:54:14 EST	10.76.225.140	0		216.58.229.238	443	CONNECT	DENIED			/	175	238	Web Ads/Analytics		FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	www.google-an	Mountain View, United States
15 Nov 2016 07:54:14 EST	10.76.225.140	0		216.58.216.238	443	CONNECT	DENIED			/	175	238	Web Ads/Analytics		FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	www.google-an	Mountain View, United States
15 Nov 2016 07:54:33 EST	10.76.225.140	0		162.247.242.18	443	CONNECT	DENIED			/	175	220	Web Ads/Analytics		FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	ssarc-nr-data.ne	, United States
15 Nov 2016 07:55:10 EST	10.76.225.140	31314	216.12.191.52	80	GET	OBSERVED	http://time.chenega.com/		/	0	360	Business/	text/html,%20chara	FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	time.chenega.c	Vermillion, United States
15 Nov 2016 07:55:45 EST	10.76.225.140	0	104.129.118.187	80	GET	OBSERVED	http://global.fncstatic.com/static/v/fn-hp/js/ag.hp.new.js	http://www.foxnews.com/	/static/v/fn-hp/js/ag.hp.new.js	79004	466	Newsy/Me	application/x-javascr	FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	global.fncstatic	Cambridge, United States
15 Nov 2016 07:55:45 EST	10.76.225.140	23505	54.230.5.78	80	GET	OBSERVED	http://d5t9c0tpq0ha1.cloudfront.net/?a=FoxNews	http://www.foxnews.com/	/?	5970	470	Content-T	image/gif	?a=FoxNe	FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	d5t9c0tpq0ha1.	Seattle, United States
15 Nov 2016 07:55:45 EST	10.76.225.140	23504	52.84.93.218	80	GET	DENIED	http://d6gt23463.mealads.com/?a=FoxNews	http://www.foxnews.com/	/	5459	353	Web Ads/	image/gif	?a=FoxNe	FIETC	Mozilla/5.0 (Windows NT 6.1; WOW64;	d6gt23463.meal	Seattle, United States
15 Nov 2016 07:55:45 EST	10.76.225.140	12026	104.129.118.187	80	GET	OBSERVED	http://a57.foxnews.com/a57.foxnews.com/scat/images	http://www.foxnews.com/	/www.foxnews.com/scat/images/121/91/3	11226

Obtained via FOIA by Judicial Watch, Inc.

| | | |

Obtained via FOIA by Judicial Watch, Inc.

Obtained via FOIA by Judicial Watch, Inc.

| | | |

Obtained via FOIA by Judicial Watch, Inc.

15 Nov 2016 23:21:40 EDT	10.76.225.140	10.245.15.188	46142	104.45.214.112	443	CONNECT	OBSERVED	tcp://nexus.officeapps.live.com/	/		4551	925	Office/Business Applications	FLETC	nexus.officeapp Redmond, United States
15 Nov 2016 23:21:40 EDT	10.76.225.140	10.245.15.188	46196	168.61.149.17	443	CONNECT	OBSERVED	tcp://nexusrules.officeapps.live.com/	/		4199	940	Office/Business Applications	FLETC	nexusrules.offic , United States

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
To:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6); (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6); (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Socdhsonenet.cbp.dhs.gov3a5>"; "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"
CC:	"/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Socdhsonenet.cbp.dhs.gov3a5>"
Subject:	RE: Georgia Case | Analysis
Date:	2016/12/10 17:14:39
Priority:	Normal
Type:	Note

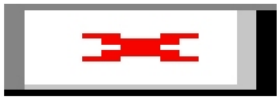
(b)(6)

The (b)(6) test was done at "10 Dec 2016 12:32:54 EDT".

Thanks,

(b)(6)

Security Analyst, SOC
General Dynamics Information Technology
Enterprise **S**ecurity **O**perations **C**enter (ESOC)
Department of Homeland Security
MGMT/OCIO/OCISO



dhs_esoc_2_info

From: (b)(6)
Sent: Saturday, December 10, 2016 3:49 PM
To: (b)(6) CTR) <(b)(6)>; (b)(6) <(b)(6)>; DHS ESOC <DHSESOC@hq.dhs.gov>; DHS ESOC Leads <DHSESOCLeads@hq.dhs.gov>
Cc: DHS ESOC Analysts <DHSESOCAnalysts@hq.dhs.gov>; DHS ESOC <DHSESOC@hq.dhs.gov>
Subject: RE: Georgia Case | Analysis

Obtained via FOIA by Judicial Watch, Inc.

Good find Andy. Just as a precautionary measure, can you jot down the exact time that you conducted this test and pull the timestamps/logs of that traffic. I have a feeling that they are on high alert and that it may have possibly caused another scan event. At least if they do come at us, we are all prepared and can show them how we recreated the issue.

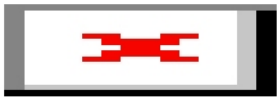
Thanks,

Sean

From: (b)(6) (CTR)
Sent: Saturday, December 10, 2016 2:42:28 PM
To: (b)(6) (b)(6) DHS ESOC; DHS ESOC Leads
Cc: DHS ESOC Analysts; DHS ESOC
Subject: RE: Georgia Case | Analysis

Will try and report back.

v/r
(b)(6) GCIH, Sec+
Security Analyst, SOC – Shift Lead
General Dynamics Information Technology
Enterprise **S**ecurity **O**perations **C**enter (ESOC)
Department of Homeland Security
MGMT/OCIO/OCISO



dhs_esoc_2_info

From: (b)(6)
Sent: Saturday, December 10, 2016 2:41 PM
To: DHS ESOC <DHSESOC@hq.dhs.gov>; DHS ESOC Leads <DHSESOCLeads@hq.dhs.gov>
Cc: DHS ESOC Analysts <DHSESOCAnalysts@hq.dhs.gov>; DHS ESOC <DHSESOC@hq.dhs.gov>
Subject: RE: (b)(6) Case | Analysis

Team --

Great bit of analysis. Quick question: can you all attempt to reproduce the HTTP OPTIONS error just through Internet Explorer? Based on our interview with the FLETC user this morning, this error occurred when he was attempting to query a web front end form via IE (version unknown at this time).

(b)(6) (b)(6)

Obtained via FOIA by Judicial Watch, Inc.

(Acting) Chief, DHS ESOC
Office of the Chief Information Security Officer
Department of Homeland Security
Mobile: 202-657-(b)(6)

From: (b)(6) (CTR) on behalf of DHS ESOC
Sent: Saturday, December 10, 2016 2:33:13 PM
To: DHS ESOC Leads
Cc: DHS ESOC Analysts; DHS ESOC
Subject: Georgia Case | Analysis

ALCON,

In an attempt to further analyze "Georgia" case, I've accidently recreated (almost exactly) the OPTIONS traffic to the "verify.sos.ga[.]gov" site.

Before I explain what steps I took to create this traffic, here is why it happened.
ESOC was contacted by FLETC wondering why there was difference in source port between Netflow from FLETC (56337) and our BlueCoat logs (63636).
We had to take few steps to explain this process and I mistakenly copy/pasted the Georgia url.
However, we ultimately did verify the difference in port translation between FLETC Netflow and BlueCoat logs. Please see attached file "Port Translation.xlsx"

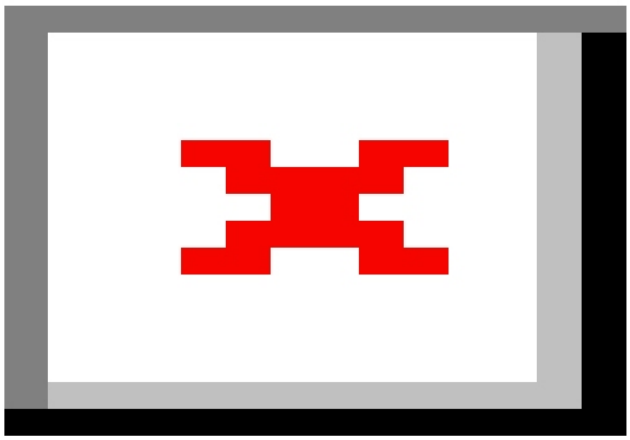
But at the same time, this "accident" explain how a Microsoft Product can possibly invoke OPTIONS traffic to certain websites and that this traffic was not malicious.
Please note in the attached Splunk logs and pcap, the User Agent String is different- "Microsoft Office Word 2013" and not "Microsoft Office Protocol Discovery"

Steps I took to create this traffic:

1. Opened a new Word document and hit "Save As" then selected a "Desktop" folder
2. In the "File name" box, I mistakenly pasted the url "hxxp://verify.sos.ga[.]gov" (without the obfuscation and was not able to grab a screenshot, but similar to one shown below) then hit "Save"

Obtained via FOIA by Judicial Watch, Inc.

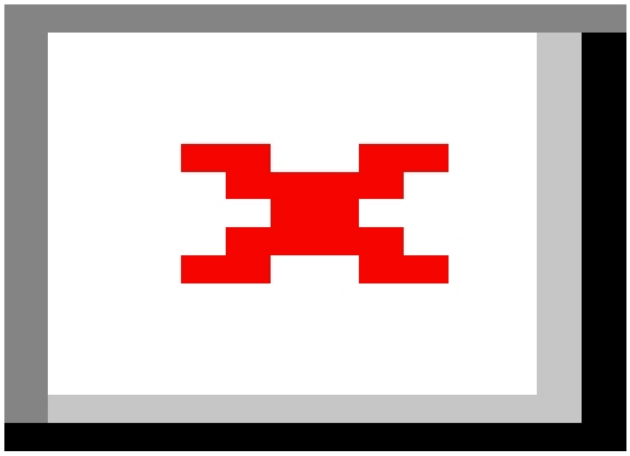
3.



4. Window message popped-up stating “connecting to “verify.sos.ga[.]gov…..” (Was not able to grab a screenshot, but similar to one shown below)

Obtained via FOIA by Judicial Watch, Inc.

5.

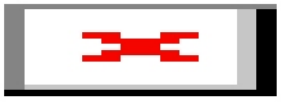


6. Once I saw this message, I pressed “Cancel” button. It did not cancel at first so I pressed the “Cancel” button three more times. At the end I had to force close Word from the Task Manager.

I’ve attached both Splunk logs and the pcap of this event.

v/r

(b)(6) GCIH, Sec+
Security Analyst, SOC – Shift Lead
General Dynamics Information Technology
Enterprise **S**ecurity **O**perations **C**enter (ESOC)
Department of Homeland Security
MGMT/OCIO/OCISO



dhs_esoc_2_info

Sender:	(b)(6) CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
Recipient:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=(b)(6)

Obtained via FOIA by Judicial Watch, Inc.

	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Socdhsonenet.cbp.dhs.gov3a5>"; "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"; "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Socdhsonenet.cbp.dhs.gov3a5>"
Sent Date:	2016/12/10 17:14:37
Delivered Date:	2016/12/10 17:14:39

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
To:	(b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"
CC:	"/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Subject:	RE: Georgia Case | Analysis
Date:	2016/12/10 17:21:44
Priority:	Normal
Type:	Note

Based on previous tests, it only allowed pdf documents upload.

V/r,
(b)(6)

From: (b)(6) (b)(6)
Sent: Saturday, December 10, 2016 5:19 PM
To: (b)(6) (b)((b)(6) (b)(6) (b)((b)(6) DHS ESOC (b)(6) DHS ESOC Leads (b)(6)
Cc: DHS ESOC Analysts (b)(6) DHS ESOC (b)(6)
Subject: RE: Georgia Case | Analysis

That is outstanding work (b)(6)

It is hard to determine if that is exactly what the FLETC user may have been doing without talking to him. However, what may have happened is the applicant hyperlinked a copy of his license certificate found on the Georgia SoS in a Microsoft Word resume and the FLETC user clicked it triggering the response.

(b)(6) can you browse the SoS site on the OOB and see if it allows users to upload documents and link back to the site to verify their certificate/license document? Might be a bit of a stretch. Let me know if you have any other leading theories.

Thanks,

(b)(6)

Obtained via FOIA by Judicial Watch, Inc.

From: (b)(6) (b)( ) (CTR)
Sent: Saturday, December 10, 2016 4:48:40 PM
To: (b)(6) (b)(6 DHS ESOC; DHS ESOC Leads
Cc: DHS ESOC Analysts; DHS ESOC
Subject: RE: Georgia Case | Analysis

(b)(6

I have been able to replicate the HTTP OPTIONS along with the same user agent "Microsoft Office Protocol Discovery" as seen with the FLETC user. See Splunk Logs.

According to Microsoft:

"

Understanding Microsoft Office Protocol Discovery

When an Office application receives a request to open a Web resource, the Office application has to make the following decisions about how to open the Web resource:

- Open the resource as read-only from the content that is downloaded by Internet Explorer. This content is opened in browse mode.

- Open the resource as read/write with a document lock on the server for exclusive access. This content is opened in edit mode.

The decision about how to open the Web resource is resolved by investigating the folder path where the document comes from and by investigating the capabilities of the server that manages that path. To determine what capabilities the server supports, Office 2003 issues an HTTP 1.1 standard OPTIONS command. The OPTIONS command requests that the server identify what commands and what methods that the server supports for the folder where the document is located. The server identification is done according to the rules that are outlined in RFC 2616. An HTTP 1.1-compatible Web server responds to the OPTIONS request with the list of methods that are supported for the uniform resource identifier (URI). Office evaluates the response and then looks for the following:" - https://support.microsoft.com/en-us/kb/838028

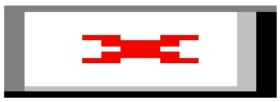
Based on that information I was able to replicate the traffic by creating an embedded link targeted at word document and upon going to the link, I saw the traffic generated by our logs.

Obtained via FOIA by Judicial Watch, Inc.



Thanks,

(b)(6)
Security Analyst, SOC
General Dynamics Information Technology
Enterprise **S**ecurity **O**perations **C**enter (ESOC)
Department of Homeland Security
MGMT/OCIO/OCISO



dhs_esoc_2_info

From: (b)(6) (b)(
Sent: Saturday, December 10, 2016 2:41 PM
To: DHS ESOC (b)(6) DHS ESOC Leads (b)(6)
Cc: DHS ESOC Analysts (b)(6) DHS ESOC (b)(6)
Subject: RE: Georgia Case | Analysis

Team --

Great bit of analysis. Quick question: can you all attempt to reproduce the HTTP OPTIONS error just through Internet Explorer? Based on our interview with the FLETC user this morning, this error occurred when he was attempting to query a web front end form via IE (version unknown at this time).

Obtained via FOIA by Judicial Watch, Inc.

(b)(6) (b)(6)
(Acting) Chief, DHS ESOC
Office of the Chief Information Security Officer
Department of Homeland Security
Mobile: 202-657-(b)(6)

From: (b)(6) (CTR) on behalf of DHS ESOC
Sent: Saturday, December 10, 2016 2:33:13 PM
To: DHS ESOC Leads
Cc: DHS ESOC Analysts; DHS ESOC
Subject: Georgia Case | Analysis

ALCON,

In an attempt to further analyze "Georgia" case, I've accidently recreated (almost exactly) the OPTIONS traffic to the "verify.sos.ga[.]gov" site.

Before I explain what steps I took to create this traffic, here is why it happened.
ESOC was contacted by FLETC wondering why there was difference in source port between Netflow from FLETC (56337) and our BlueCoat logs (63636).
We had to take few steps to explain this process and I mistakenly copy/pasted the Georgia url.
However, we ultimately did verify the difference in port translation between FLETC Netflow and BlueCoat logs. Please see attached file "Port Translation.xlsx"

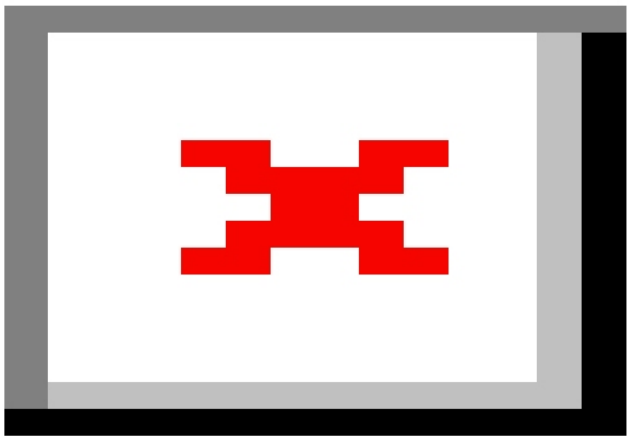
But at the same time, this "accident" explain how a Microsoft Product can possibly invoke OPTIONS traffic to certain websites and that this traffic was not malicious.
Please note in the attached Splunk logs and pcap, the User Agent String is different- "Microsoft Office Word 2013" and not "Microsoft Office Protocol Discovery"

Steps I took to create this traffic:

1. Opened a new Word document and hit "Save As" then selected a "Desktop" folder
2. In the "File name" box, I mistakenly pasted the url "hxxp://verify.sos.ga[.]gov" (without the obfuscation and was not able to grab a screenshot, but similar to one shown below) then hit "Save"

Obtained via FOIA by Judicial Watch, Inc.

3.

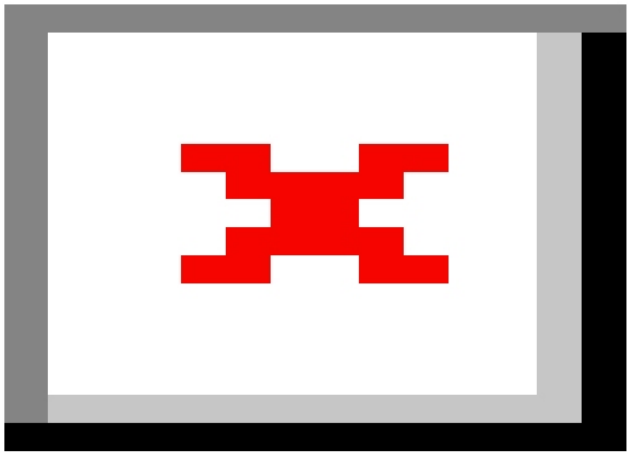


cid:image004.jpg@01D252FB.CD809270

4. Window message popped-up stating “connecting to “verify.sos.ga[.]gov…..” (Was not able to grab a screenshot, but similar to one shown below)

Obtained via FOIA by Judicial Watch, Inc.

5.

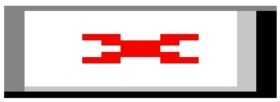


cid:image005.jpg@01D252FB.CD809270

6. Once I saw this message, I pressed “Cancel” button. It did not cancel at first so I pressed the “Cancel” button three more times. At the end I had to force close Word from the Task Manager.

I’ve attached both Splunk logs and the pcap of this event.

v/r
(b)(6) (b)(6) GCIH, Sec+
Security Analyst, SOC – Shift Lead
General Dynamics Information Technology
Enterprise **S**ecurity **O**perations **C**enter (ESOC)
Department of Homeland Security
MGMT/OCIO/OCISO



dhs_esoc_2_info

Sender:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Recipient:	(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP

Obtained via FOIA by Judicial Watch, Inc.

	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"; "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Sent Date:	2016/12/10 17:21:42
Delivered Date:	2016/12/10 17:21:44

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
To:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
CC:	(b)(6) (b)(6 (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6 (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6 (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Subject:	RE: Georgia Event Analysis
Date:	2016/12/12 08:40:55
Priority:	Normal
Type:	Note

(b)(6) –

This is perfect. Thanks for the quick turnaround.

(b)((b)(6)
(Acting) Chief, DHS ESOC
Office of the Chief Information Security Officer
Department of Homeland Security
Mobile: 202-657-(b)(6)

From: (b)(6) (b)(6) M
Sent: Monday, December 12, 2016 8:31 AM
To: (b)(6) (b)((b)(6)
Cc: (b)(6) (b)(6) (CTR) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) >; (b)(6) (b)((b)(6) (b)(6) (b)(6) (b)(6) (b)(6 (b)((b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (CTR) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6)

Obtained via FOIA by Judicial Watch, Inc.

(CTR) (b)(6) (b)(6) (b)(6) (CTR)
(b)(6) Rohner, Boyden (b)(6) (b)(6)
(b)(6) (b)(6) (b)(6) (b)(6) (b)(6)
Subject: RE: Georgia Event Analysis

(b)(6)

Below is a listing of software installed on the computer systems. This report was pulled from System Center Configuration Manager (SCCM). Additionally, this table is located in the ONENOTE document I uploaded to the SEN. Please let me know if you need anything else.

Name	Company	Version
Cisco AnyConnect Secure Mobility Client	Cisco Systems, Inc.	4.3.02039
CyberLink PowerDVD 9.5	CyberLink Corp.	9.5.1.3426
Microsoft Office Professional Plus 2013	Microsoft Corporation	15.0.4569.1506
Microsoft SQL Server Compact 3.5 SP2 ENU	Microsoft Corporation	3.5.8080.0
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation	8.0.61001
Microsoft Office Professional Plus 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Access MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Excel MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft PowerPoint MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Publisher MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Outlook MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Word MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Office Proofing Tools 2013 - English	Microsoft Corporation	15.0.4569.1506
Outils de vérification linguistique 2013 de Microsoft Office - Français	Microsoft Corporation	15.0.4569.1506
Microsoft Office Proofing Tools 2013 - Español	Microsoft Corporation	15.0.4569.1506
Microsoft Office Proofing (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft InfoPath MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Office Shared MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft DCF MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft OneNote MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Groove MUI (English) 2013	Microsoft Corporation	15.0.4569.1506

Obtained via FOIA by Judicial Watch, Inc.

Microsoft Office OSM MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Office OSM UX MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Office Shared Setup Metadata MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Access Setup Metadata MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Lync MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
CyberLink PowerDVD 9.5	CyberLink Corp.	9.5.1.3426
Adobe Acrobat DC	Adobe Systems Incorporated	15.006.30198
Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030	Microsoft Corporation	11.0.61030.0
McAfee VirusScan Enterprise	McAfee, Inc.	8.8.08000
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	Microsoft Corporation	10.0.40219
DYMO Label v.8	Sanford, L.P.	8.5.0.1751
PELCO DX Series Client	PELCO	2.01.0036
Identiv uTrust Velocity 3.6.0	Identiv	03.05.030.174
Topaz e-Signatures SigPlus 4.4.0.6	Topaz Systems, Inc.	4.4.0.6
Microsoft Interop Forms Redistributable Package 2.0a	Microsoft Corporation	2.0.0
Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022	Microsoft Corporation	9.0.21022
Citrix Receiver	Citrix Systems, Inc.	14.1.0.0
Citrix Receiver(Aero)	Citrix Systems, Inc.	14.1.0.0
Citrix Receiver(USB)	Citrix Systems, Inc.	14.1.0.0
Self-service Plug-in	Citrix Systems, Inc.	4.1.0.41738
Citrix Receiver(DV)	Citrix Systems, Inc.	14.1.0.0
Citrix Receiver (HDX Flash Redirection)	Citrix Systems, Inc.	14.1.0.0
Citrix Authentication Manager	Citrix Systems, Inc.	5.1.0.62606
Citrix Receiver Inside	Citrix Systems, Inc.	4.1.0.56471
Online Plug-in	Citrix Systems, Inc.	14.1.0.0

Obtained via FOIA by Judicial Watch, Inc.

McAfee Policy Auditor Agent	McAfee, Inc.	6.2.0.276
Carbon Black Sensor	Carbon Black, Inc	5.1.0.51215
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005	Microsoft Corporation	12.0.21005
Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030	Microsoft Corporation	11.0.61030.0
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030	Microsoft Corporation	11.0.61030
Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030	Microsoft Corporation	11.0.61030
DS	Pelco	7.10.247.10443
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501	Microsoft Corporation	12.0.30501.0
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005	Microsoft Corporation	12.0.21005
Citrix Online Launcher	Citrix	1.0.408
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	Microsoft Corporation	9.0.30729.4148
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	Microsoft Corporation	9.0.30729.6161
Adobe Flash Player 22 ActiveX	Adobe Systems Incorporated	22.0.0.210
Adobe Flash Player 22 NPAPI	Adobe Systems Incorporated	22.0.0.209
FletcWarn	DHS.FLETC	1.3
Cisco AnyConnect Diagnostics and Reporting Tool	Cisco Systems, Inc.	4.3.02039
Cisco AnyConnect Secure Mobility Client	Cisco Systems, Inc.	4.3.02039
Cisco AnyConnect Start Before Login Module	Cisco Systems, Inc.	4.3.02039
VLC media player	VideoLAN	2.2.4
DS ControlPoint	Pelco	7.15.70.11007
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	Microsoft Corporation	10.0.40219
Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030	Microsoft Corporation	11.0.61030

Obtained via FOIA by Judicial Watch, Inc.

Configuration Manager Client	Microsoft Corporation	5.00.7958.1000
Microsoft Silverlight	Microsoft Corporation	5.1.50901.0
Dell Data Protection | Encryption	Dell Inc	8.4.1.6428
Microsoft Office 64-bit Components 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Office Shared 64-bit MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2013	Microsoft Corporation	15.0.4569.1506
Microsoft Policy Platform	Microsoft Corporation	1.2.3602.0
Microsoft .NET Framework 4.6.1	Microsoft Corporation	4.6.01055
Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005	Microsoft Corporation	12.0.21005
Microsoft Visual C++ 2005 Redistributable (x64)	Microsoft Corporation	8.0.61000
Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030	Microsoft Corporation	11.0.61030
McAfee Host Intrusion Prevention	McAfee, Inc.	8.00.0801
McAfee Host Intrusion Prevention	McAfee, Inc.	8.00.0801
Microsoft SQL Server Compact 3.5 SP2 x64 ENU	Microsoft Corporation	3.5.8080.0
1E Agent	1E	6.5.100
DX Series Client		
Microsoft SQL Server Native Client	Microsoft Corporation	9.00.2047.00
Microsoft SQL Server 2005 Backward compatibility	Microsoft Corporation	8.05.2309
Microsoft SQL Server 2008 Native Client	Microsoft Corporation	10.0.1600.22
64 Bit HP CIO Components Installer	Hewlett-Packard	15.2.1
Monitor Information Reporting v5	Enhansoft	5.01.4
Microsoft .NET Framework 4.6.1	Microsoft Corporation	4.6.01055
Microsoft Visual C++ 2008 Redistributable - x64 9.0.21022	Microsoft Corporation	9.0.21022
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	Microsoft Corporation	9.0.30729.6161
McAfee Agent	McAfee, Inc.	5.0.4.283
McAfee Client Proxy	McAfee	2.2.1.107

Obtained via FOIA by Judicial Watch, Inc.

R/
(b)(6) (b)(6) |THE FLETC|912-267-2700

From: (b)(6) (b)(
Sent: Monday, December 12, 2016 8:01 AM
To: (b)(6) (b)(6) M (b)(6)
Cc: DHS ESOC Leads (b)(6)
Subject: Georgia Event Analysis

(b)(6)

If you could get me some sort of software inventory from the workstation in question (OS, applications installed, versions, etc.), that would be a huge help. I'm going to have a meeting today with Microsoft SMEs to discuss what the technical causes of this event could have been, and I suspect they will want to know a lot of this kind of information.

Thanks in advance and let me know if you have any questions.

(b)((b)(6)
(Acting) Chief, DHS ESOC
Office of the Chief Information Security Officer
Department of Homeland Security
Mobile: 202-657-7024

Sender:	(b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Recipient:	(b)(6) (b)(6) M </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6 (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6 (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6 </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6 (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Sent Date:	2016/12/12 08:40:54

Obtained via FOIA by Judicial Watch, Inc.

Delivered Date:	2016/12/12 08:40:55

Obtained via FOIA by Judicial Watch, Inc.

sIP	dIP	sPort	dPort	pro	packets	bytes	flags	sTime	duration	eTime	sensor
50.232.155.145	216.81.94.70	80	32112	6	12	12233	SRPA	2016/02/02T14:39:14.072	127.031	2016/02/02T14:41:21.103	STENNIS4
50.232.155.145	216.81.94.70	80	32188	6	3	1557	SRPA	2016/02/02T14:39:14.531	126.572	2016/02/02T14:41:21.103	STENNIS4
50.232.155.145	216.81.94.70	80	64731	6	93	125764	SRPA	2016/02/02T14:42:44.516	217.058	2016/02/02T14:46:21.574	STENNIS4
50.232.155.145	216.81.81.85	80	10960	6	2	505	S PA	2016/02/02T14:34:49.371	0.075	2016/02/02T14:34:49.446	DHSCV4
50.232.155.145	216.81.81.85	80	10979	6	7	9060	S A	2016/02/02T14:34:49.445	0.089	2016/02/02T14:34:49.534	DHSCV4
50.232.155.145	216.81.81.85	80	11017	6	124	163624	SRPA	2016/02/02T14:34:49.531	256.349	2016/02/02T14:39:05.880	DHSCV4
216.81.94.70	50.232.155.145	32112	80	6	9	1090	S PA	2016/02/02T14:39:14.015	127.088	2016/02/02T14:41:21.103	STENNIS4
216.81.94.70	50.232.155.145	32188	80	6	4	734	S PA	2016/02/02T14:39:14.474	126.629	2016/02/02T14:41:21.103	STENNIS4
216.81.94.70	50.232.155.145	64731	80	6	67	13851	S PA	2016/02/02T14:42:44.459	217.115	2016/02/02T14:46:21.574	STENNIS4
216.81.81.85	50.232.155.145	10960	80	6	4	656	SRPA	2016/02/02T14:34:49.336	0.110	2016/02/02T14:34:49.446	DHSCV4
216.81.81.85	50.232.155.145	10979	80	6	6	540	FSRPA	2016/02/02T14:34:49.410	0.124	2016/02/02T14:34:49.534	DHSCV4
216.81.81.85	50.232.155.145	10979	80	6	1	40	R	2016/02/02T14:34:49.534	0.000	2016/02/02T14:34:49.534	DHSCV4
216.81.81.85	50.232.155.145	11017	80	6	93	20225	S PA	2016/02/02T14:34:49.497	256.383	2016/02/02T14:39:05.880	DHSCV4
50.232.155.145	216.81.81.85	80	12641	6	59	76960	SRPA	2016/02/02T16:11:18.987	145.937	2016/02/02T16:13:44.924	DHSCV4
216.81.81.85	50.232.155.145	12641	80	6	44	11276	S PA	2016/02/02T16:11:18.952	145.972	2016/02/02T16:13:44.924	DHSCV4
50.232.155.145	216.81.94.71	80	7105	6	3	2110	S PA	2016/02/02T19:03:40.384	46.484	2016/02/02T19:04:26.868	STENNIS4
50.232.155.145	216.81.94.71	80	7003	6	20	25791	SRPA	2016/02/02T19:03:39.984	131.359	2016/02/02T19:05:51.343	STENNIS4
50.232.155.145	216.81.94.71	80	7103	6	103	135220	SRPA	2016/02/02T19:03:40.376	176.037	2016/02/02T19:06:36.413	STENNIS4
50.232.155.145	216.81.94.71	80	15414	6	3	1557	SRPA	2016/02/02T19:04:26.868	129.545	2016/02/02T19:06:36.413	STENNIS4
50.232.155.145	216.81.94.71	80	7106	6	4	3014	SRPA	2016/02/02T19:03:40.387	176.026	2016/02/02T19:06:36.413	STENNIS4
50.232.155.145	216.81.94.71	80	42488	6	18	23230	SRPA	2016/02/02T19:07:09.969	131.720	2016/02/02T19:09:21.689	STENNIS4
50.232.155.145	216.81.81.83	80	6282	6	14	15151	SRPA	2016/02/02T19:04:11.330	130.048	2016/02/02T19:06:21.378	DHSCV4
50.232.155.145	216.81.81.83	80	43714	6	114	143270	SRPA	2016/02/02T19:06:39.623	212.132	2016/02/02T19:10:11.755	DHSCV4
50.232.155.145	216.81.81.83	80	63797	6	4	3014	SRPA	2016/02/02T19:08:00.420	131.335	2016/02/02T19:10:11.755	DHSCV4
216.81.94.71	50.232.155.145	7105	80	6	5	1323	SRPA	2016/02/02T19:03:40.327	46.541	2016/02/02T19:04:26.868	STENNIS4
216.81.94.71	50.232.155.145	7003	80	6	16	2779	S PA	2016/02/02T19:03:39.927	131.416	2016/02/02T19:05:51.343	STENNIS4
216.81.94.71	50.232.155.145	7103	80	6	86	24142	S PA	2016/02/02T19:03:40.318	176.095	2016/02/02T19:06:36.413	STENNIS4
216.81.94.71	50.232.155.145	15414	80	6	4	471	S PA	2016/02/02T19:04:26.810	129.603	2016/02/02T19:06:36.413	STENNIS4
216.81.94.71	50.232.155.145	7106	80	6	6	2536	S PA	2016/02/02T19:03:40.329	176.084	2016/02/02T19:06:36.413	STENNIS4
216.81.94.71	50.232.155.145	42488	80	6	14	2963	S PA	2016/02/02T19:07:09.910	131.779	2016/02/02T19:09:21.689	STENNIS4
216.81.81.83	50.232.155.145	6282	80	6	12	4033	S PA	2016/02/02T19:04:11.296	130.082	2016/02/02T19:06:21.378	DHSCV4
216.81.81.83	50.232.155.145	43714	80	6	81	15094	S PA	2016/02/02T19:06:39.591	212.164	2016/02/02T19:10:11.755	DHSCV4
216.81.81.83	50.232.155.145	63797	80	6	5	1304	S PA	2016/02/02T19:08:00.387	131.368	2016/02/02T19:10:11.755	DHSCV4

Obtained via FOIA by Judicial Watch, Inc.

sIP	dIP	sPort	dPort	pro	packets	bytes	flags	sTime	duration	eTime	sensor
50.232.155.145	216.81.94.73	80	59612	6	17	20366	FS PA	2016/02/28T08:22:18.580	127.715	2016/02/28T08:24:26.295	STENNIS4
50.232.155.145	216.81.94.73	80	59603	6	22	28959	SRPA	2016/02/28T08:22:18.323	131.382	2016/02/28T08:24:29.705	STENNIS4
50.232.155.145	216.81.94.73	80	59614	6	3	1557	SRPA	2016/02/28T08:22:18.603	131.101	2016/02/28T08:24:29.704	STENNIS4
50.232.155.145	216.81.94.73	80	59613	6	77	103411	SRPA	2016/02/28T08:22:18.604	266.328	2016/02/28T08:26:44.932	STENNIS4
216.81.94.73	50.232.155.145	59612	80	6	15	4196	FSRPA	2016/02/28T08:22:18.524	127.771	2016/02/28T08:24:26.295	STENNIS4
216.81.94.73	50.232.155.145	59603	80	6	16	1724	S PA	2016/02/28T08:22:18.268	131.437	2016/02/28T08:24:29.705	STENNIS4
216.81.94.73	50.232.155.145	59614	80	6	4	1212	S PA	2016/02/28T08:22:18.549	131.155	2016/02/28T08:24:29.704	STENNIS4
216.81.94.73	50.232.155.145	59613	80	6	65	18094	S PA	2016/02/28T08:22:18.548	266.384	2016/02/28T08:26:44.932	STENNIS4

Obtained via FOIA by Judicial Watch, Inc.

sIP	dIP	sPort	dPort	pro	packets	bytes	flags	sTime	duration	eTime	sensor
50.232.155.157	216.81.81.80	80	34039	6	3	257	FS PA	2016/05/23T11:02:07.836	0.055	2016/05/23T11:02:07.891	DHSCV4
50.232.155.157	216.81.81.80	80	34041	6	3	257	FS PA	2016/05/23T11:02:07.846	0.055	2016/05/23T11:02:07.901	DHSCV4
50.232.155.157	216.81.81.80	80	34028	6	201	295803	S PA	2016/05/23T11:02:07.729	2.067	2016/05/23T11:02:09.796	DHSCV4
50.232.155.157	216.81.81.80	80	34029	6	87	127893	S PA	2016/05/23T11:02:07.737	2.106	2016/05/23T11:02:09.843	DHSCV4
50.232.155.157	216.81.81.80	80	34230	6	3	256	FS PA	2016/05/23T11:02:09.796	0.073	2016/05/23T11:02:09.869	DHSCV4
50.232.155.157	216.81.81.80	80	34240	6	3	257	FS PA	2016/05/23T11:02:09.848	0.055	2016/05/23T11:02:09.903	DHSCV4
50.232.155.157	216.81.81.80	80	34241	6	3	257	FS PA	2016/05/23T11:02:09.848	0.055	2016/05/23T11:02:09.903	DHSCV4
50.232.155.157	216.81.81.80	80	34289	6	5	4156	FS PA	2016/05/23T11:02:10.449	0.058	2016/05/23T11:02:10.507	DHSCV4
50.232.155.157	216.81.81.80	80	33995	6	91	133598	S PA	2016/05/23T11:02:07.086	2.762	2016/05/23T11:02:09.848	DHSCV4
50.232.155.157	216.81.81.80	80	34237	6	3	257	FS PA	2016/05/23T11:02:09.842	0.055	2016/05/23T11:02:09.897	DHSCV4
50.232.155.157	216.81.81.80	80	34242	6	3	257	FS PA	2016/05/23T11:02:09.849	0.055	2016/05/23T11:02:09.904	DHSCV4
50.232.155.157	216.81.81.80	80	34266	6	6	812	SRPA	2016/05/23T11:02:10.113	168.185	2016/05/23T11:04:58.298	DHSCV4
216.81.81.80	50.232.155.157	34039	80	6	5	604	FS PA	2016/05/23T11:02:07.810	0.081	2016/05/23T11:02:07.891	DHSCV4
216.81.81.80	50.232.155.157	34041	80	6	5	601	FS PA	2016/05/23T11:02:07.820	0.081	2016/05/23T11:02:07.901	DHSCV4
216.81.81.80	50.232.155.157	34028	80	6	134	7860	SRPA	2016/05/23T11:02:07.703	2.093	2016/05/23T11:02:09.796	DHSCV4
216.81.81.80	50.232.155.157	34029	80	6	60	4013	SRPA	2016/05/23T11:02:07.710	2.133	2016/05/23T11:02:09.843	DHSCV4
216.81.81.80	50.232.155.157	34230	80	6	5	601	FS PA	2016/05/23T11:02:09.769	0.100	2016/05/23T11:02:09.869	DHSCV4
216.81.81.80	50.232.155.157	34240	80	6	5	609	FS PA	2016/05/23T11:02:09.822	0.081	2016/05/23T11:02:09.903	DHSCV4
216.81.81.80	50.232.155.157	34241	80	6	5	608	FS PA	2016/05/23T11:02:09.822	0.081	2016/05/23T11:02:09.903	DHSCV4
216.81.81.80	50.232.155.157	34289	80	6	6	616	FSRPA	2016/05/23T11:02:10.423	0.084	2016/05/23T11:02:10.507	DHSCV4
216.81.81.80	50.232.155.157	33995	80	6	72	5487	SRPA	2016/05/23T11:02:07.059	2.789	2016/05/23T11:02:09.848	DHSCV4
216.81.81.80	50.232.155.157	34237	80	6	5	603	FS PA	2016/05/23T11:02:09.816	0.081	2016/05/23T11:02:09.897	DHSCV4
216.81.81.80	50.232.155.157	34242	80	6	5	602	FS PA	2016/05/23T11:02:09.822	0.082	2016/05/23T11:02:09.904	DHSCV4
216.81.81.80	50.232.155.157	34266	80	6	8	4496	S PA	2016/05/23T11:02:10.086	168.212	2016/05/23T11:04:58.298	DHSCV4
50.232.155.157	216.81.94.72	80	15809	6	14	18157	S PA	2016/05/23T12:42:02.923	0.739	2016/05/23T12:42:03.662	STENNIS4
50.232.155.157	216.81.94.72	80	15939	6	3	257	FS PA	2016/05/23T12:42:03.668	0.087	2016/05/23T12:42:03.755	STENNIS4
50.232.155.157	216.81.94.72	80	15940	6	3	257	FS PA	2016/05/23T12:42:03.672	0.087	2016/05/23T12:42:03.759	STENNIS4
50.232.155.157	216.81.94.72	80	15941	6	3	257	FS PA	2016/05/23T12:42:03.674	0.087	2016/05/23T12:42:03.761	STENNIS4
50.232.155.157	216.81.94.72	80	15937	6	3	257	FS PA	2016/05/23T12:42:03.662	0.087	2016/05/23T12:42:03.749	STENNIS4
50.232.155.157	216.81.94.72	80	15942	6	3	257	FS PA	2016/05/23T12:42:03.674	0.087	2016/05/23T12:42:03.761	STENNIS4
50.232.155.157	216.81.94.72	80	15944	6	3	257	FS PA	2016/05/23T12:42:03.683	0.087	2016/05/23T12:42:03.770	STENNIS4
50.232.155.157	216.81.94.72	80	15943	6	3	257	FS PA	2016/05/23T12:42:03.683	0.087	2016/05/23T12:42:03.770	STENNIS4
50.232.155.157	216.81.94.72	80	15985	6	26	21297	S PA	2016/05/23T12:42:03.969	123.697	2016/05/23T12:44:07.666	STENNIS4
50.232.155.157	216.81.94.72	80	35779	6	3	257	FS PA	2016/05/23T12:44:07.666	0.089	2016/05/23T12:44:07.755	STENNIS4
50.232.155.157	216.81.94.72	80	15986	6	44	46592	S PA	2016/05/23T12:42:03.981	129.368	2016/05/23T12:44:13.349	STENNIS4
50.232.155.157	216.81.94.72	80	36802	6	13	17000	S PA	2016/05/23T12:44:13.615	0.391	2016/05/23T12:44:14.006	STENNIS4
50.232.155.157	216.81.94.72	80	36859	6	3	257	FS PA	2016/05/23T12:44:14.006	0.087	2016/05/23T12:44:14.093	STENNIS4
50.232.155.157	216.81.94.72	80	36765	6	7	9060	S A	2016/05/23T12:44:13.349	0.268	2016/05/23T12:44:13.617	STENNIS4
50.232.155.157	216.81.94.72	80	36867	6	3	257	FS PA	2016/05/23T12:44:14.060	0.086	2016/05/23T12:44:14.146	STENNIS4
50.232.155.157	216.81.94.72	80	36986	6	3	256	FS PA	2016/05/23T12:44:14.633	0.101	2016/05/23T12:44:14.734	STENNIS4
50.232.155.157	216.81.94.72	80	36998	6	3	257	FS PA	2016/05/23T12:44:14.659	0.087	2016/05/23T12:44:14.746	STENNIS4
50.232.155.157	216.81.94.72	80	36999	6	3	257	FS PA	2016/05/23T12:44:14.659	0.087	2016/05/23T12:44:14.746	STENNIS4
50.232.155.157	216.81.94.72	80	36985	6	12	1880	SRPA	2016/05/23T12:44:14.626	188.506	2016/05/23T12:47:23.132	STENNIS4
50.232.155.157	216.81.94.72	80	45827	6	6	812	SRPA	2016/05/23T12:45:08.694	134.438	2016/05/23T12:47:23.132	STENNIS4
216.81.94.72	50.232.155.157	15809	80	6	13	1176	SRPA	2016/05/23T12:42:02.881	0.781	2016/05/23T12:42:03.662	STENNIS4
216.81.94.72	50.232.155.157	15939	80	6	5	605	FS PA	2016/05/23T12:42:03.626	0.129	2016/05/23T12:42:03.755	STENNIS4
216.81.94.72	50.232.155.157	15940	80	6	5	602	FS PA	2016/05/23T12:42:03.630	0.129	2016/05/23T12:42:03.759	STENNIS4
216.81.94.72	50.232.155.157	15941	80	6	5	599	FS PA	2016/05/23T12:42:03.632	0.129	2016/05/23T12:42:03.761	STENNIS4
216.81.94.72	50.232.155.157	15937	80	6	5	602	FS PA	2016/05/23T12:42:03.620	0.129	2016/05/23T12:42:03.749	STENNIS4
216.81.94.72	50.232.155.157	15942	80	6	5	601	FS PA	2016/05/23T12:42:03.633	0.128	2016/05/23T12:42:03.761	STENNIS4
216.81.94.72	50.232.155.157	15944	80	6	5	601	FS PA	2016/05/23T12:42:03.641	0.129	2016/05/23T12:42:03.770	STENNIS4
216.81.94.72	50.232.155.157	15943	80	6	5	603	FS PA	2016/05/23T12:42:03.641	0.129	2016/05/23T12:42:03.770	STENNIS4
216.81.94.72	50.232.155.157	15985	80	6	30	14545	SRPA	2016/05/23T12:42:03.927	123.739	2016/05/23T12:44:07.666	STENNIS4
216.81.94.72	50.232.155.157	35779	80	6	5	605	FS PA	2016/05/23T12:44:07.624	0.131	2016/05/23T12:44:07.755	STENNIS4
216.81.94.72	50.232.155.157	15986	80	6	44	18362	SRPA	2016/05/23T12:42:03.938	129.411	2016/05/23T12:44:13.349	STENNIS4
216.81.94.72	50.232.155.157	36802	80	6	12	2012	SRPA	2016/05/23T12:44:13.573	0.433	2016/05/23T12:44:14.006	STENNIS4
216.81.94.72	50.232.155.157	36859	80	6	5	601	FS PA	2016/05/23T12:44:13.964	0.129	2016/05/23T12:44:14.093	STENNIS4
216.81.94.72	50.232.155.157	36765	80	6	6	542	FSRPA	2016/05/23T12:44:13.306	0.311	2016/05/23T12:44:13.617	STENNIS4
216.81.94.72	50.232.155.157	36867	80	6	5	604	FS PA	2016/05/23T12:44:14.017	0.129	2016/05/23T12:44:14.146	STENNIS4
216.81.94.72	50.232.155.157	36986	80	6	5	601	FS PA	2016/05/23T12:44:14.591	0.143	2016/05/23T12:44:14.734	STENNIS4
216.81.94.72	50.232.155.157	36998	80	6	5	608	FS PA	2016/05/23T12:44:14.617	0.129	2016/05/23T12:44:14.746	STENNIS4
216.81.94.72	50.232.155.157	36999	80	6	5	609	FS PA	2016/05/23T12:44:14.617	0.129	2016/05/23T12:44:14.746	STENNIS4
216.81.94.72	50.232.155.157	36985	80	6	17	10445	S PA	2016/05/23T12:44:14.583	188.549	2016/05/23T12:47:23.132	STENNIS4
216.81.94.72	50.232.155.157	45827	80	6	8	4327	S PA	2016/05/23T12:45:08.652	134.480	2016/05/23T12:47:23.132	STENNIS4
50.232.155.157	216.81.94.69	80	18464	6	3	531	FS PA	2016/05/23T13:42:08.831	0.085	2016/05/23T13:42:08.916	STENNIS4
50.232.155.157	216.81.94.69	80	18536	6	2	479	S PA	2016/05/23T13:42:09.081	0.159	2016/05/23T13:42:09.240	STENNIS4
50.232.155.157	216.81.94.69	80	18570	6	8	8302	FS PA	2016/05/23T13:42:09.239	0.092	2016/05/23T13:42:09.331	STENNIS4
50.232.155.157	216.81.94.69	80	18599	6	13	16440	S PA	2016/05/23T13:42:09.329	0.976	2016/05/23T13:42:10.305	STENNIS4
50.232.155.157	216.81.94.69	80	18811	6	3	257	FS PA	2016/05/23T13:42:10.304	0.086	2016/05/23T13:42:10.390	STENNIS4
50.232.155.157	216.81.94.69	80	18812	6	3	257	FS PA	2016/05/23T13:42:10.309	0.086	2016/05/23T13:42:10.395	STENNIS4
50.232.155.157	216.81.94.69	80	18813	6	3	257	FS PA	2016/05/23T13:42:10.309	0.086	2016/05/23T13:42:10.395	STENNIS4
50.232.155.157	216.81.94.69	80	18829	6	3	257	FS PA	2016/05/23T13:42:10.371	0.086	2016/05/23T13:42:10.457	STENNIS4
50.232.155.157	216.81.94.69	80	18814	6	3	257	FS PA	2016/05/23T13:42:10.310	0.085	2016/05/23T13:42:10.395	STENNIS4
50.232.155.157	216.81.94.69	80	18817	6	3	257	FS PA	2016/05/23T13:42:10.325	0.086	2016/05/23T13:42:10.411	STENNIS4
50.232.155.157	216.81.94.69	80	19021	6	4	4104	S PA	2016/05/23T13:42:11.041	0.087	2016/05/23T13:42:11.128	STENNIS4
50.232.155.157	216.81.94.69	80	19021	6	1	52	F A	2016/05/23T13:42:11.128	0.000	2016/05/23T13:42:11.128	STENNIS4
50.232.155.157	216.81.94.69	80	18984	6	3	404	SRPA	2016/05/23T13:42:10.895	132.761	2016/05/23T13:44:23.656	STENNIS4
50.232.155.157	216.81.94.69	80	18994	6	3	404	SRPA	2016/05/23T13:42:10.944	132.712	2016/05/23T13:44:23.656	STENNIS4
216.81.94.69	50.232.155.157	18464	80	6	5	464	FS PA	2016/05/23T13:42:08.790	0.126	2016/05/23T13:42:08.916	STENNIS4
216.81.94.69	50.232.155.157	18536	80	6	5	689	SRPA	2016/05/23T13:42:09.039	0.201	2016/05/23T13:42:09.240	STENNIS4
216.81.94.69	50.232.155.157	18570	80	6	6	527	FSRPA	2016/05/23T13:42:09.196	0.135	2016/05/23T13:42:09.331	STENNIS4
216.81.94.69	50.232.155.157	18599	80	6	13	1461	SRPA	2016/05/23T13:42:09.287	1.018	2016/05/23T13:42:10.305	STENNIS4

Obtained via FOIA by Judicial Watch, Inc.

216.81.94.69	50.232.155.157	18811	80	6	5	602	FS PA	2016/05/23T13:42:10.263	0.127	2016/05/23T13:42:10.390	STENNIS4
216.81.94.69	50.232.155.157	18812	80	6	5	601	FS PA	2016/05/23T13:42:10.268	0.127	2016/05/23T13:42:10.395	STENNIS4
216.81.94.69	50.232.155.157	18813	80	6	5	599	FS PA	2016/05/23T13:42:10.268	0.127	2016/05/23T13:42:10.395	STENNIS4
216.81.94.69	50.232.155.157	18829	80	6	5	602	FS PA	2016/05/23T13:42:10.330	0.127	2016/05/23T13:42:10.457	STENNIS4
216.81.94.69	50.232.155.157	18814	80	6	5	603	FS PA	2016/05/23T13:42:10.269	0.126	2016/05/23T13:42:10.395	STENNIS4
216.81.94.69	50.232.155.157	18817	80	6	5	605	FS PA	2016/05/23T13:42:10.284	0.127	2016/05/23T13:42:10.411	STENNIS4
216.81.94.69	50.232.155.157	19021	80	6	6	615	FSRPA	2016/05/23T13:42:11.000	0.128	2016/05/23T13:42:11.128	STENNIS4
216.81.94.69	50.232.155.157	19021	80	6	1	40	R	2016/05/23T13:42:11.128	0.000	2016/05/23T13:42:11.128	STENNIS4
216.81.94.69	50.232.155.157	18984	80	6	4	961	S PA	2016/05/23T13:42:10.854	132.802	2016/05/23T13:44:23.656	STENNIS4
216.81.94.69	50.232.155.157	18994	80	6	4	1047	S PA	2016/05/23T13:42:10.903	132.753	2016/05/23T13:44:23.656	STENNIS4
50.232.155.157	216.81.81.80	80	53188	6	14	17583	S PA	2016/05/23T14:43:03.434	5.685	2016/05/23T14:43:09.119	DHSCV4
50.232.155.157	216.81.81.80	80	54548	6	3	257	FS PA	2016/05/23T14:43:09.347	0.055	2016/05/23T14:43:09.402	DHSCV4
50.232.155.157	216.81.81.80	80	54560	6	3	257	FS PA	2016/05/23T14:43:09.440	0.055	2016/05/23T14:43:09.495	DHSCV4
50.232.155.157	216.81.81.80	80	54489	6	57	82170	SRPA	2016/05/23T14:43:09.118	130.521	2016/05/23T14:45:19.639	DHSCV4
216.81.81.80	50.232.155.157	53188	80	6	13	1813	SRPA	2016/05/23T14:43:03.408	5.711	2016/05/23T14:43:09.119	DHSCV4
216.81.81.80	50.232.155.157	54548	80	6	5	601	FS PA	2016/05/23T14:43:09.321	0.081	2016/05/23T14:43:09.402	DHSCV4
216.81.81.80	50.232.155.157	54560	80	6	5	604	FS PA	2016/05/23T14:43:09.414	0.081	2016/05/23T14:43:09.495	DHSCV4
216.81.81.80	50.232.155.157	54489	80	6	39	2363	S PA	2016/05/23T14:43:09.092	130.547	2016/05/23T14:45:19.639	DHSCV4
50.232.155.157	216.81.94.73	80	60958	6	2	491	S PA	2016/05/23T18:16:42.075	0.358	2016/05/23T18:16:42.433	STENNIS4
50.232.155.157	216.81.94.73	80	61284	6	16	19105	S PA	2016/05/23T18:16:43.196	12.116	2016/05/23T18:16:55.312	STENNIS4
50.232.155.157	216.81.94.73	80	63723	6	3	257	FS PA	2016/05/23T18:16:55.311	0.323	2016/05/23T18:16:55.634	STENNIS4
50.232.155.157	216.81.94.73	80	63958	6	3	257	FS PA	2016/05/23T18:16:56.416	0.357	2016/05/23T18:16:56.773	STENNIS4
50.232.155.157	216.81.94.73	80	63987	6	2	322	S PA	2016/05/23T18:16:56.601	5.185	2016/05/23T18:17:01.786	STENNIS4
50.232.155.157	216.81.94.73	80	65342	6	3	257	FS PA	2016/05/23T18:17:01.785	0.366	2016/05/23T18:17:02.151	STENNIS4
50.232.155.157	216.81.94.73	80	65398	6	3	257	FS PA	2016/05/23T18:17:02.004	0.358	2016/05/23T18:17:02.362	STENNIS4
50.232.155.157	216.81.94.73	80	65468	6	3	257	FS PA	2016/05/23T18:17:02.247	0.383	2016/05/23T18:17:02.630	STENNIS4
50.232.155.157	216.81.94.73	80	1047	6	3	257	FS PA	2016/05/23T18:17:02.530	0.348	2016/05/23T18:17:02.878	STENNIS4
50.232.155.157	216.81.94.73	80	1688	6	4	560	S PA	2016/05/23T18:17:05.112	17.632	2016/05/23T18:17:22.744	STENNIS4
50.232.155.157	216.81.94.73	80	5937	6	3	257	FS PA	2016/05/23T18:17:22.743	0.343	2016/05/23T18:17:23.086	STENNIS4
50.232.155.157	216.81.94.73	80	61029	6	3	606	SRPA	2016/05/23T18:16:42.433	128.358	2016/05/23T18:18:50.791	STENNIS4
50.232.155.157	216.81.94.73	80	6393	6	3	404	SRPA	2016/05/23T18:17:24.414	126.448	2016/05/23T18:19:30.862	STENNIS4
216.81.94.73	50.232.155.157	60958	80	6	5	593	SRPA	2016/05/23T18:16:41.911	0.522	2016/05/23T18:16:42.433	STENNIS4
216.81.94.73	50.232.155.157	61284	80	6	18	2422	SRPA	2016/05/23T18:16:43.020	12.292	2016/05/23T18:16:55.312	STENNIS4
216.81.94.73	50.232.155.157	63723	80	6	5	601	FS PA	2016/05/23T18:16:55.152	0.482	2016/05/23T18:16:55.634	STENNIS4
216.81.94.73	50.232.155.157	63958	80	6	5	604	FS PA	2016/05/23T18:16:56.244	0.529	2016/05/23T18:16:56.773	STENNIS4
216.81.94.73	50.232.155.157	63987	80	6	5	738	SRPA	2016/05/23T18:16:56.423	5.363	2016/05/23T18:17:01.786	STENNIS4
216.81.94.73	50.232.155.157	65342	80	6	5	603	FS PA	2016/05/23T18:17:01.613	0.538	2016/05/23T18:17:02.151	STENNIS4
216.81.94.73	50.232.155.157	65398	80	6	5	601	FS PA	2016/05/23T18:17:01.823	0.539	2016/05/23T18:17:02.362	STENNIS4
216.81.94.73	50.232.155.157	65468	80	6	5	609	FS PA	2016/05/23T18:17:02.073	0.557	2016/05/23T18:17:02.630	STENNIS4
216.81.94.73	50.232.155.157	1047	80	6	5	608	FS PA	2016/05/23T18:17:02.350	0.528	2016/05/23T18:17:02.878	STENNIS4
216.81.94.73	50.232.155.157	1688	80	6	7	1563	SRPA	2016/05/23T18:17:04.919	17.825	2016/05/23T18:17:22.744	STENNIS4
216.81.94.73	50.232.155.157	5937	80	6	5	605	FS PA	2016/05/23T18:17:22.558	0.528	2016/05/23T18:17:23.086	STENNIS4
216.81.94.73	50.232.155.157	61029	80	6	4	441	S PA	2016/05/23T18:16:42.254	128.537	2016/05/23T18:18:50.791	STENNIS4
216.81.94.73	50.232.155.157	6393	80	6	4	923	S PA	2016/05/23T18:17:24.244	126.618	2016/05/23T18:19:30.862	STENNIS4
50.232.155.157	216.81.94.68	80	2615	6	190	278950	SRPA	2016/05/23T19:14:22.932	128.593	2016/05/23T19:16:31.525	STENNIS4
50.232.155.157	216.81.94.68	80	2567	6	7	7080	SRPA	2016/05/23T19:14:22.744	128.782	2016/05/23T19:16:31.526	STENNIS4
50.232.155.157	216.81.94.68	80	2389	6	120	174654	SRPA	2016/05/23T19:14:22.087	129.438	2016/05/23T19:16:31.525	STENNIS4
50.232.155.157	216.81.94.68	80	2613	6	58	83584	SRPA	2016/05/23T19:14:22.929	128.596	2016/05/23T19:16:31.525	STENNIS4
50.232.155.157	216.81.94.68	80	2565	6	18	22771	SRPA	2016/05/23T19:14:22.743	128.783	2016/05/23T19:16:31.526	STENNIS4
50.232.155.157	216.81.94.68	80	2564	6	14	16804	SRPA	2016/05/23T19:14:22.742	128.784	2016/05/23T19:16:31.526	STENNIS4
50.232.155.157	216.81.94.68	80	2614	6	89	128195	SRPA	2016/05/23T19:14:22.931	133.619	2016/05/23T19:16:36.550	STENNIS4
50.232.155.157	216.81.94.68	80	2573	6	74	105420	SRPA	2016/05/23T19:14:22.756	133.794	2016/05/23T19:16:36.550	STENNIS4
50.232.155.157	216.81.94.68	80	2612	6	72	102347	SRPA	2016/05/23T19:14:22.929	133.621	2016/05/23T19:16:36.550	STENNIS4
50.232.155.157	216.81.94.68	80	2611	6	85	122031	SRPA	2016/05/23T19:14:22.924	133.626	2016/05/23T19:16:36.550	STENNIS4
50.232.155.157	216.81.94.68	80	2618	6	63	86004	SRPA	2016/05/23T19:14:22.941	138.607	2016/05/23T19:16:41.548	STENNIS4
50.232.155.157	216.81.81.82	80	42759	6	3	257	FS PA	2016/05/23T19:15:08.729	0.058	2016/05/23T19:15:08.787	DHSCV4
50.232.155.157	216.81.81.82	80	42705	6	86	122178	SRPA	2016/05/23T19:15:08.530	127.854	2016/05/23T19:17:16.384	DHSCV4
50.232.155.157	216.81.81.82	80	42710	6	90	128222	SRPA	2016/05/23T19:15:08.531	127.853	2016/05/23T19:17:16.384	DHSCV4
50.232.155.157	216.81.81.82	80	42804	6	72	105013	SRPA	2016/05/23T19:15:08.916	127.468	2016/05/23T19:17:16.384	DHSCV4
50.232.155.157	216.81.81.82	80	42797	6	59	85052	SRPA	2016/05/23T19:15:08.908	127.476	2016/05/23T19:17:16.384	DHSCV4
50.232.155.157	216.81.81.82	80	42602	6	84	119355	SRPA	2016/05/23T19:15:08.016	128.368	2016/05/23T19:17:16.384	DHSCV4
50.232.155.157	216.81.81.82	80	42807	6	3	245	SRPA	2016/05/23T19:15:08.942	127.442	2016/05/23T19:17:16.384	DHSCV4
50.232.155.157	216.81.81.82	80	42794	6	71	102200	SRPA	2016/05/23T19:15:08.896	127.488	2016/05/23T19:17:16.384	DHSCV4
50.232.155.157	216.81.81.82	80	42800	6	113	162263	SRPA	2016/05/23T19:15:08.910	132.481	2016/05/23T19:17:21.391	DHSCV4
216.81.94.68	50.232.155.157	2615	80	6	129	7589	S PA	2016/05/23T19:14:22.717	128.808	2016/05/23T19:16:31.525	STENNIS4
216.81.94.68	50.232.155.157	2567	80	6	6	1206	S PA	2016/05/23T19:14:22.536	128.990	2016/05/23T19:16:31.526	STENNIS4
216.81.94.68	50.232.155.157	2389	80	6	80	5673	S PA	2016/05/23T19:14:21.872	129.653	2016/05/23T19:16:31.525	STENNIS4
216.81.94.68	50.232.155.157	2613	80	6	39	2910	S PA	2016/05/23T19:14:22.714	128.811	2016/05/23T19:16:31.525	STENNIS4
216.81.94.68	50.232.155.157	2565	80	6	14	1595	S PA	2016/05/23T19:14:22.536	128.990	2016/05/23T19:16:31.526	STENNIS4
216.81.94.68	50.232.155.157	2564	80	6	12	2357	S PA	2016/05/23T19:14:22.533	128.993	2016/05/23T19:16:31.526	STENNIS4
216.81.94.68	50.232.155.157	2614	80	6	59	4916	S PA	2016/05/23T19:14:22.716	133.834	2016/05/23T19:16:36.550	STENNIS4
216.81.94.68	50.232.155.157	2573	80	6	53	5572	S PA	2016/05/23T19:14:22.549	134.001	2016/05/23T19:16:36.550	STENNIS4
216.81.94.68	50.232.155.157	2612	80	6	50	4455	S PA	2016/05/23T19:14:22.714	133.836	2016/05/23T19:16:36.550	STENNIS4
216.81.94.68	50.232.155.157	2611	80	6	60	4975	S PA	2016/05/23T19:14:22.710	133.840	2016/05/23T19:16:36.550	STENNIS4
216.81.94.68	50.232.155.157	2618	80	6	48	7603	S PA	2016/05/23T19:14:22.723	138.825	2016/05/23T19:16:41.548	STENNIS4
216.81.81.82	50.232.155.157	42759	80	6	5	608	FS PA	2016/05/23T19:15:08.701	0.086	2016/05/23T19:15:08.787	DHSCV4
216.81.81.82	50.232.155.157	42705	80	6	61	6089	S PA	2016/05/23T19:15:08.502	127.882	2016/05/23T19:17:16.384	DHSCV4
216.81.81.82	50.232.155.157	42710	80	6	62	6152	S PA	2016/05/23T19:15:08.504	127.880	2016/05/23T19:17:16.384	DHSCV4
216.81.81.82	50.232.155.157	42804	80	6	47	3358	S PA	2016/05/23T19:15:08.888	127.496	2016/05/23T19:17:16.384	DHSCV4
216.81.81.82	50.232.155.157	42797	80	6	40	2995	S PA	2016/05/23T19:15:08.880	127.504	2016/05/23T19:17:16.384	DHSCV4
216.81.81.82	50.232.155.157	42602	80	6	59	6563	S PA	2016/05/23T19:15:07.988	128.396	2016/05/23T19:17:16.384	DHSCV4
216.81.81.82	50.232.155.157	42807	80	6	4	1217	S PA	2016/05/23T19:15:08.915	127.469	2016/05/23T19:17:16.384	DHSCV4
216.81.81.82	50.232.155.157	42794	80	6	48	3411	S PA	2016/05/23T19:15:08.868	127.516	2016/05/23T19:17:16.384	DHSCV4

Obtained via FOIA by Judicial Watch, Inc.

216.81.81.82	50.232.155.157	42800	80	6	77	7947	S PA	2016/05/23T19:15:08.882	132.509	2016/05/23T19:17:21.391	DHSCV4
50.232.155.157	216.81.94.73	80	38370	6	15	17752	S PA	2016/05/23T22:20:00.371	0.728	2016/05/23T22:20:01.099	STENNIS4
50.232.155.157	216.81.94.73	80	38413	6	9	11327	S PA	2016/05/23T22:20:00.859	0.240	2016/05/23T22:20:01.099	STENNIS4
50.232.155.157	216.81.94.73	80	38432	6	3	257	FS PA	2016/05/23T22:20:01.099	0.085	2016/05/23T22:20:01.184	STENNIS4
50.232.155.157	216.81.94.73	80	38433	6	3	257	FS PA	2016/05/23T22:20:01.099	0.085	2016/05/23T22:20:01.184	STENNIS4
50.232.155.157	216.81.94.73	80	38440	6	3	257	FS PA	2016/05/23T22:20:01.131	0.084	2016/05/23T22:20:01.215	STENNIS4
50.232.155.157	216.81.94.73	80	38451	6	3	257	FS PA	2016/05/23T22:20:01.184	0.085	2016/05/23T22:20:01.269	STENNIS4
50.232.155.157	216.81.94.73	80	38449	6	3	257	FS PA	2016/05/23T22:20:01.167	0.084	2016/05/23T22:20:01.251	STENNIS4
50.232.155.157	216.81.94.73	80	38448	6	3	257	FS PA	2016/05/23T22:20:01.167	0.084	2016/05/23T22:20:01.251	STENNIS4
50.232.155.157	216.81.94.73	80	38472	6	3	375	FS PA	2016/05/23T22:20:01.456	0.117	2016/05/23T22:20:01.573	STENNIS4
50.232.155.157	216.81.94.73	80	38477	6	15	15902	S PA	2016/05/23T22:20:01.506	16.956	2016/05/23T22:20:18.462	STENNIS4
50.232.155.157	216.81.94.73	80	40203	6	3	375	FS PA	2016/05/23T22:20:18.403	0.085	2016/05/23T22:20:18.488	STENNIS4
50.232.155.157	216.81.94.73	80	40208	6	3	257	FS PA	2016/05/23T22:20:18.462	0.085	2016/05/23T22:20:18.547	STENNIS4
50.232.155.157	216.81.94.73	80	40209	6	3	257	FS PA	2016/05/23T22:20:18.465	0.085	2016/05/23T22:20:18.550	STENNIS4
50.232.155.157	216.81.94.73	80	40214	6	3	257	FS PA	2016/05/23T22:20:18.505	0.088	2016/05/23T22:20:18.593	STENNIS4
50.232.155.157	216.81.94.73	80	40215	6	3	375	FS PA	2016/05/23T22:20:18.508	0.085	2016/05/23T22:20:18.593	STENNIS4
50.232.155.157	216.81.94.73	80	40216	6	3	257	FS PA	2016/05/23T22:20:18.508	0.085	2016/05/23T22:20:18.593	STENNIS4
50.232.155.157	216.81.94.73	80	40217	6	3	257	FS PA	2016/05/23T22:20:18.512	0.086	2016/05/23T22:20:18.598	STENNIS4
50.232.155.157	216.81.94.73	80	38471	6	3	416	S PA	2016/05/23T22:20:01.452	16.951	2016/05/23T22:20:18.403	STENNIS4
50.232.155.157	216.81.94.73	80	40206	6	3	257	FS PA	2016/05/23T22:20:18.462	0.084	2016/05/23T22:20:18.546	STENNIS4
50.232.155.157	216.81.94.73	80	40207	6	3	257	FS PA	2016/05/23T22:20:18.462	0.085	2016/05/23T22:20:18.547	STENNIS4
50.232.155.157	216.81.94.73	80	40212	6	3	257	FS PA	2016/05/23T22:20:18.488	0.096	2016/05/23T22:20:18.584	STENNIS4
50.232.155.157	216.81.94.73	80	40213	6	3	375	FS PA	2016/05/23T22:20:18.498	0.086	2016/05/23T22:20:18.584	STENNIS4
50.232.155.157	216.81.94.73	80	40211	6	3	257	FS PA	2016/05/23T22:20:18.485	0.099	2016/05/23T22:20:18.584	STENNIS4
50.232.155.157	216.81.94.73	80	40235	6	6	812	SRPA	2016/05/23T22:20:18.661	191.153	2016/05/23T22:23:29.814	STENNIS4
50.232.155.157	216.81.94.73	80	40230	6	80	110533	SRPA	2016/05/23T22:20:18.611	196.199	2016/05/23T22:23:34.810	STENNIS4
50.232.155.157	216.81.94.73	80	55935	6	3	404	SRPA	2016/05/23T22:32:12.325	128.543	2016/05/23T22:34:20.868	STENNIS4
50.232.155.157	216.81.94.73	80	55934	6	3	404	SRPA	2016/05/23T22:32:12.325	128.543	2016/05/23T22:34:20.868	STENNIS4
50.232.155.157	216.81.81.85	80	8663	6	3	3008	S PA	2016/05/23T22:36:24.831	0.093	2016/05/23T22:36:24.924	DHSCV4
50.232.155.157	216.81.81.85	80	8665	6	4	3573	S PA	2016/05/23T22:36:24.836	0.136	2016/05/23T22:36:24.972	DHSCV4
50.232.155.157	216.81.81.85	80	8617	6	45	62461	S PA	2016/05/23T22:36:24.179	0.803	2016/05/23T22:36:24.982	DHSCV4
50.232.155.157	216.81.81.85	80	8673	6	3	257	FS PA	2016/05/23T22:36:24.923	0.061	2016/05/23T22:36:24.984	DHSCV4
50.232.155.157	216.81.81.85	80	8679	6	3	257	FS PA	2016/05/23T22:36:24.982	0.060	2016/05/23T22:36:25.042	DHSCV4
50.232.155.157	216.81.81.85	80	8681	6	3	257	FS PA	2016/05/23T22:36:24.985	0.061	2016/05/23T22:36:25.046	DHSCV4
50.232.155.157	216.81.81.85	80	8660	6	7	8379	S PA	2016/05/23T22:36:24.817	0.106	2016/05/23T22:36:24.923	DHSCV4
50.232.155.157	216.81.81.85	80	8674	6	3	257	FS PA	2016/05/23T22:36:24.924	0.060	2016/05/23T22:36:24.984	DHSCV4
50.232.155.157	216.81.81.85	80	8677	6	3	257	FS PA	2016/05/23T22:36:24.972	0.060	2016/05/23T22:36:25.032	DHSCV4
50.232.155.157	216.81.81.85	80	8684	6	3	257	FS PA	2016/05/23T22:36:24.989	0.061	2016/05/23T22:36:25.050	DHSCV4
50.232.155.157	216.81.81.85	80	8692	6	3	404	SRPA	2016/05/23T22:36:25.129	131.152	2016/05/23T22:38:36.281	DHSCV4
50.232.155.157	216.81.81.85	80	8693	6	3	404	SRPA	2016/05/23T22:36:25.129	131.152	2016/05/23T22:38:36.281	DHSCV4
216.81.94.73	50.232.155.157	38370	80	6	13	1531	SRPA	2016/05/23T22:20:00.330	0.769	2016/05/23T22:20:01.099	STENNIS4
216.81.94.73	50.232.155.157	38413	80	6	10	1493	SRPA	2016/05/23T22:20:00.818	0.281	2016/05/23T22:20:01.099	STENNIS4
216.81.94.73	50.232.155.157	38432	80	6	5	599	FS PA	2016/05/23T22:20:01.058	0.126	2016/05/23T22:20:01.184	STENNIS4
216.81.94.73	50.232.155.157	38433	80	6	5	605	FS PA	2016/05/23T22:20:01.058	0.126	2016/05/23T22:20:01.184	STENNIS4
216.81.94.73	50.232.155.157	38440	80	6	5	601	FS PA	2016/05/23T22:20:01.089	0.126	2016/05/23T22:20:01.215	STENNIS4
216.81.94.73	50.232.155.157	38451	80	6	5	602	FS PA	2016/05/23T22:20:01.143	0.126	2016/05/23T22:20:01.269	STENNIS4
216.81.94.73	50.232.155.157	38449	80	6	5	602	FS PA	2016/05/23T22:20:01.126	0.125	2016/05/23T22:20:01.251	STENNIS4
216.81.94.73	50.232.155.157	38448	80	6	5	603	FS PA	2016/05/23T22:20:01.126	0.125	2016/05/23T22:20:01.251	STENNIS4
216.81.94.73	50.232.155.157	38472	80	6	5	580	FS PA	2016/05/23T22:20:01.415	0.158	2016/05/23T22:20:01.573	STENNIS4
216.81.94.73	50.232.155.157	38477	80	6	13	2069	SRPA	2016/05/23T22:20:01.465	16.997	2016/05/23T22:20:18.462	STENNIS4
216.81.94.73	50.232.155.157	40203	80	6	5	594	FS PA	2016/05/23T22:20:18.362	0.126	2016/05/23T22:20:18.488	STENNIS4
216.81.94.73	50.232.155.157	40208	80	6	5	600	FS PA	2016/05/23T22:20:18.421	0.126	2016/05/23T22:20:18.547	STENNIS4
216.81.94.73	50.232.155.157	40209	80	6	5	602	FS PA	2016/05/23T22:20:18.424	0.126	2016/05/23T22:20:18.550	STENNIS4
216.81.94.73	50.232.155.157	40214	80	6	5	591	FS PA	2016/05/23T22:20:18.464	0.129	2016/05/23T22:20:18.593	STENNIS4
216.81.94.73	50.232.155.157	40215	80	6	5	597	FS PA	2016/05/23T22:20:18.467	0.126	2016/05/23T22:20:18.593	STENNIS4
216.81.94.73	50.232.155.157	40216	80	6	5	594	FS PA	2016/05/23T22:20:18.467	0.126	2016/05/23T22:20:18.593	STENNIS4
216.81.94.73	50.232.155.157	40217	80	6	5	602	FS PA	2016/05/23T22:20:18.471	0.127	2016/05/23T22:20:18.598	STENNIS4
216.81.94.73	50.232.155.157	38471	80	6	5	1043	SRPA	2016/05/23T22:20:01.410	16.993	2016/05/23T22:20:18.403	STENNIS4
216.81.94.73	50.232.155.157	40206	80	6	5	603	FS PA	2016/05/23T22:20:18.421	0.125	2016/05/23T22:20:18.546	STENNIS4
216.81.94.73	50.232.155.157	40207	80	6	5	601	FS PA	2016/05/23T22:20:18.421	0.126	2016/05/23T22:20:18.547	STENNIS4
216.81.94.73	50.232.155.157	40212	80	6	5	599	FS PA	2016/05/23T22:20:18.447	0.137	2016/05/23T22:20:18.584	STENNIS4
216.81.94.73	50.232.155.157	40213	80	6	5	595	FS PA	2016/05/23T22:20:18.457	0.127	2016/05/23T22:20:18.584	STENNIS4
216.81.94.73	50.232.155.157	40211	80	6	5	605	FS PA	2016/05/23T22:20:18.444	0.140	2016/05/23T22:20:18.584	STENNIS4
216.81.94.73	50.232.155.157	40235	80	6	6	2151	S PA	2016/05/23T22:20:18.619	191.195	2016/05/23T22:23:29.814	STENNIS4
216.81.94.73	50.232.155.157	40230	80	6	55	5320	S PA	2016/05/23T22:20:18.570	196.240	2016/05/23T22:23:34.810	STENNIS4
216.81.94.73	50.232.155.157	55935	80	6	4	1091	S PA	2016/05/23T22:32:12.284	128.584	2016/05/23T22:34:20.868	STENNIS4
216.81.94.73	50.232.155.157	55934	80	6	4	1091	S PA	2016/05/23T22:32:12.284	128.584	2016/05/23T22:34:20.868	STENNIS4
216.81.81.85	50.232.155.157	8663	80	6	5	850	SRPA	2016/05/23T22:36:24.802	0.122	2016/05/23T22:36:24.924	DHSCV4
216.81.81.85	50.232.155.157	8665	80	6	5	922	SRPA	2016/05/23T22:36:24.807	0.165	2016/05/23T22:36:24.972	DHSCV4
216.81.81.85	50.232.155.157	8617	80	6	34	3521	SRPA	2016/05/23T22:36:24.149	0.833	2016/05/23T22:36:24.982	DHSCV4
216.81.81.85	50.232.155.157	8673	80	6	5	599	FS PA	2016/05/23T22:36:24.894	0.090	2016/05/23T22:36:24.984	DHSCV4
216.81.81.85	50.232.155.157	8679	80	6	5	602	FS PA	2016/05/23T22:36:24.953	0.089	2016/05/23T22:36:25.042	DHSCV4
216.81.81.85	50.232.155.157	8681	80	6	5	602	FS PA	2016/05/23T22:36:24.956	0.090	2016/05/23T22:36:25.046	DHSCV4
216.81.81.85	50.232.155.157	8660	80	6	8	1089	SRPA	2016/05/23T22:36:24.788	0.135	2016/05/23T22:36:24.923	DHSCV4
216.81.81.85	50.232.155.157	8674	80	6	5	605	FS PA	2016/05/23T22:36:24.895	0.089	2016/05/23T22:36:24.984	DHSCV4
216.81.81.85	50.232.155.157	8677	80	6	5	603	FS PA	2016/05/23T22:36:24.943	0.089	2016/05/23T22:36:25.032	DHSCV4
216.81.81.85	50.232.155.157	8684	80	6	5	601	FS PA	2016/05/23T22:36:24.961	0.089	2016/05/23T22:36:25.050	DHSCV4
216.81.81.85	50.232.155.157	8692	80	6	4	1091	S PA	2016/05/23T22:36:25.100	131.181	2016/05/23T22:38:36.281	DHSCV4
216.81.81.85	50.232.155.157	8693	80	6	4	1091	S PA	2016/05/23T22:36:25.100	131.181	2016/05/23T22:38:36.281	DHSCV4

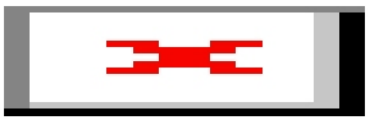
Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
To:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"
CC:	(b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Subject:	RE: Georgia Timeline Splunk Logs
Date:	2016/12/14 12:02:59
Priority:	Normal
Type:	Note

All,

Attached are the E1 results from 28 Feb 2016. There was traffic at the noted time, 1919 UTC.

R,
(b)(6) (b)(6
Information Security Analyst
General Dynamics Information Technology (GDIT)
Supporting the Department of Homeland Security (DHS)
MGMT/OCIO/CISO/SOC
DHS ESOC Main Line: 1-877-347-(b)(6)
DHS ESOC COOP: (540) 542-(b)(6)



cid:image001.png@01D15F3E.16F9DD60

From: (b)(6) (b)(6) (CTR)
Sent: Wednesday, December 14, 2016 3:09 AM
To: (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) Tran, (b)(6) (b)((CTR) (b)(6) DHS ESOC Analysts (b)(6)
Cc: (b)(6) (b)((b)(6) Rohner, Boyden (b)(6) (b)(6)

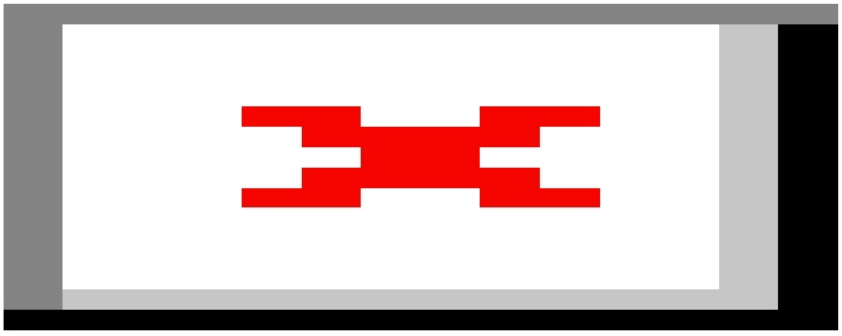
Obtained via FOIA by Judicial Watch, Inc.

(b)(6) (CTR) (b)(6)
Subject: RE: Georgia Timeline Splunk Logs

Alcon,

From the Einstein search, the below highlighted Netflow data matches the Feb 2nd and May 23rd events. Traffic is over TCP/80 and is seen going through Stennis4 E1 sensor. Although there was data for Feb 28th, traffic did not match the 13:19 CST time. Note that Netflow data does not show the HTTP Request Method. For correlation, one (1) hour was added for the different time zone, and UTC was taken into account (+4 hrs for CDT, +5 hrs for CST). Einstein results are attached and SEN Number 2016-12-093 updated. Also, in speaking with ESOC Engineering (Lavar) earlier this evening, he could not provide proxy logs for February and May, as Blue Coat data retention on their log server only goes back to November, and that our tools (Splunk) actually retains the data longer.

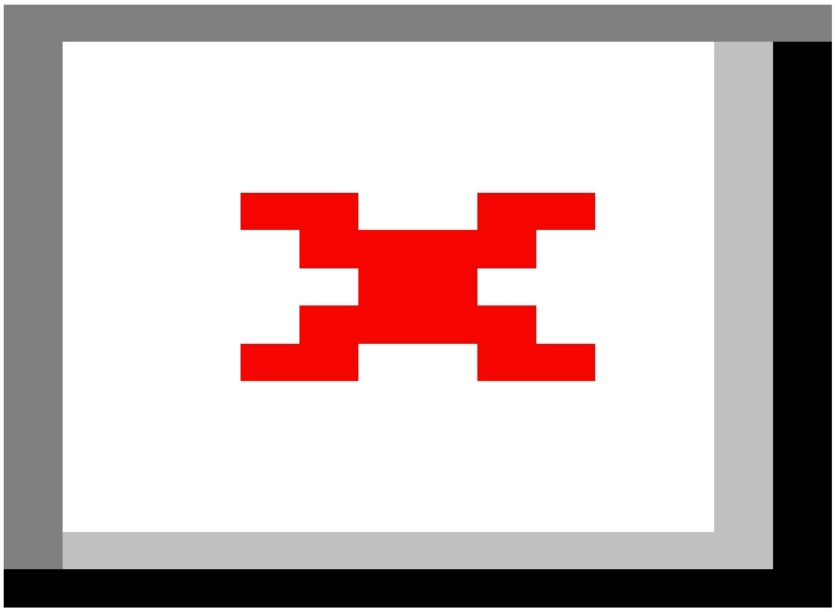
February 2nd 13:03 CST +1 =14:03 + 5 = **19:03 UTC** (hits)



February 28th 13:19 CST +1 =14:19 + 5 = **19:19 UTC** (no hits)

May 23rd 08:42 CDT +1 =09:42 + 4 = **13:42 UTC** (hits)

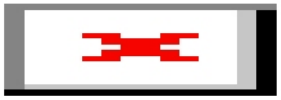
Obtained via FOIA by Judicial Watch, Inc.



V/r,

(b)(6)
Shift lead, SOC – Incident Handling
General Dynamics Information Technology (GDIT)
Supporting the Department of Homeland Security (DHS)
DHS Enterprise Security Operations Center (ESOC)
MGMT/OCIO/CISO/ESOC

Obtained via FOIA by Judicial Watch, Inc.



dhs_esoc_2_info

From: (b)(6) (b)(6) (CTR)
Sent: Wednesday, December 14, 2016 1:56 AM
To: (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) Tran, (b)(6) (b)((CTR) (b)(6) DHS ESOC Analysts (b)(6)
Cc: (b)(6) (b)((b)(6) Rohner, Boyden (b)(6) (b)(6) (b)(6) (CTR) (b)(6)
Subject: RE: Georgia Timeline Splunk Logs

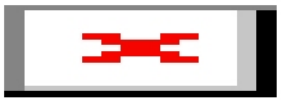
Alcon,

Currently, we have identified six (6) DHS IPs belonging to the following components (1 USCIS, 3 ICE, 1 FEMA, 1 FLETC) from September through November 2016. Searches are ongoing to identify traffic and component IPs involved in February and May.

10.61.22.222 - CIS
10.56.189.94 - ICE
10.101.194.178 - ICE
10.32.82.42 - FEMA
10.56.189.65 - ICE
10.243.15.188 - FLETC

V/r,

(b)(6) (b)(6)
Shift lead, SOC – Incident Handling
General Dynamics Information Technology (GDIT)
Supporting the Department of Homeland Security (DHS)
DHS Enterprise Security Operations Center (ESOC)
MGMT/OCIO/CISO/ESOC



dhs_esoc_2_info

From: (b)(6) (b)(6)
Sent: Tuesday, December 13, 2016 9:17 PM
To: (b)(6) (b)(6) (b)(6) Tran, (b)(6) (b)((CTR)

Obtained via FOIA by Judicial Watch, Inc.

(b)(6) DHS ESOC Analysts (b)(6)
Cc: (b)(6) (b)((b)(6) Rohner, Boyden (b)(6) (b)(6)
(b)(6) (CTR) (b)(6)
Subject: RE: Georgia Timeline Splunk Logs

Hey (b)(6)

These all match the timeline exactly. We will continue to search (b)(6) is seeing what if he can dredge up old Splunk data.

Respectfully,

(b)(6)

From: (b)(6) (b)(6)
Sent: Tuesday, December 13, 2016 9:10 PM
To: (b)(6) (b)(6) (b)((CTR) (b)(6) (b)(6) (b)(6)
(b)(6) DHS ESOC Analysts (b)(6)
Cc: (b)(6) (b)((b)(6) Rohner, Boyden (b)(6) (b)(6)
(b)(6) (CTR) (b)(6)
Subject: RE: Georgia Timeline Splunk Logs

Thanks (b)(6) Can you match this up with the timestamps in the letter? Then evaluate the e1 netflow for the oldest dates.

v/r

(b)(6)

From: (b)(6) (b)(6) (b)((CTR)
Sent: Tuesday, December 13, 2016 9:06:10 PM
To: (b)(6) (b)(6) DHS ESOC Analysts
Cc: (b)(6) (b)(6 (b)(6) (b)(6) Rohner, Boyden; (b)(6) (b)(6) (CTR)
Subject: RE: Georgia Timeline Splunk Logs

All,

Reviewing the logs (thanks (b)(6) I see nothing unusually and all attempts to Georgia's website were the same as the ones we've seen in before.

September 12, 2016 12:52:32 EDT
Host **10.61.22.222** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.georgia.gov/ (Denied)

September 28, 2016 08:54:15 EDT

Obtained via FOIA by Judicial Watch, Inc.

Host **10.56.189.94** (ICE-CIS) attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://sos.ga.gov/index.php/licensing/plb/ (Denied)

October 3, 2016 11:41:32 EDT
Host **10.101.194.178** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.state.ga.us/corporations/ (Denied)

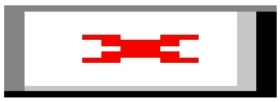
October 6, 2016 11:14:16 EDT
Host **10.32.82.42** (FEMA)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://verify.sos.ga.gov/verification/stylesheets/ (Observed)

November 7, 2016 13:15:43 EDT
Host **10.56.189.65** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.georgia.gov/plb/cosmetology/ (Denied)

November 8, 2016 08:35:21 EDT
Host **10.243.15.188** (FLETC)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://verify.sos.ga.gov/verification/stylesheets/ (Observed)

V/r,

(b)(6) (b)(6) (b)(6)
IT Security Analyst - Monitoring and Analysis
Critical Solutions LLC
Enterprise Security Operations Center (ESOC)
Department of Homeland Security
MGMT/OCIO/CISO/SOC



dhs_esoc_2_info

From: (b)(6) (b)(6)
Sent: Tuesday, December 13, 2016 8:43 PM
To: DHS ESOC Analysts (b)(6)
Cc: (b)(6) (b)((b)(6) (b)(6) (b)(6) (b)(6) Rohner, Boyden (b)(6) (b)(6) (b)(6) (CTR) (b)(6)
Subject: Georgia Timeline Splunk Logs

Team,

Attached are the Splunk logs. We will probably need to do Einstein to capture the Feb and May dates.

Used the following Splunk Seach Criteria:

index=bluecoat sourcetype=bluecoat:proxysg:access:file r_ip="50.232.155.128/24" http_method="OPTIONS" |convert timeformat="%d %b %Y %H:%M:%S EDT" ctime(_time) AS Time| sort

Obtained via FOIA by Judicial Watch, Inc.

0 -_time | rename src_ip as "Device Address", src as "Source IP", r_ip as "Destination IP", cs_uri_port as "Destination Port", s_source_port as "Source Port", http_method as "Request Method",status as "Status Code", sc_filter_result as "Device Action", url as "Request URL", cs_Referer as "Request Referrer", cs_uri_path as "Request URL File Name" , bytes_in as "Bytes In", bytes_out as "Bytes Out", category as "Request Domain Category", http_content_type as "Request File Type", cs_uri_query as "Request Query", s_hierarchy as "Component", http_user_agent as "Request User Agent", dest_host as "Request URL Host" | iplocation "Destination IP" | eval "Destination Geo Address"=City+", "+Country | table Time, "Device Address", "Source IP" ,"Source Port", "Destination IP" ,"Destination Port", "Request Method","Status Code", "Device Action", "Request URL", "Request Referrer", "Request URL File Name", "Bytes In", "Bytes Out", "Request Domain Category", "Request File Type" , "Request Query", "Component" , "Request User Agent", "Request URL Host", "Destination Geo Address"

Respectfully,

(b)(6) (b)(6)

Sender:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Recipient:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Sent Date:	2016/12/14 12:02:58
Delivered Date:	2016/12/14 12:02:59

Obtained via FOIA by Judicial Watch, Inc.

sIP	dIP	sPort	dPort	pro	packets	bytes	flags	sTime	duration	eTime	sensor
216.81.94.73	50.232.155.133	56787	80	6	33	4609	S PA	2016/02/28T08:20:18.035	161.242	2016/02/28T08:22:59.277	STENNIS4
50.232.155.133	216.81.94.73	80	56787	6	44	60232	SRPA	2016/02/28T08:20:18.091	161.186	2016/02/28T08:22:59.277	STENNIS4
216.81.94.73	50.232.155.146	57370	443	6	22	3657	FS PA	2016/02/28T08:20:46.803	79.821	2016/02/28T08:22:06.624	STENNIS4
50.232.155.146	216.81.94.73	443	57370	6	19	21210	FS PA	2016/02/28T08:20:46.860	79.764	2016/02/28T08:22:06.624	STENNIS4
216.81.94.73	50.232.155.146	57406	443	6	15	2216	FS PA	2016/02/28T08:20:48.047	78.577	2016/02/28T08:22:06.624	STENNIS4
216.81.94.73	50.232.155.146	57409	443	6	8	1303	FS PA	2016/02/28T08:20:48.049	78.574	2016/02/28T08:22:06.623	STENNIS4
216.81.94.73	50.232.155.146	57408	443	6	12	2060	FS PA	2016/02/28T08:20:48.049	78.575	2016/02/28T08:22:06.624	STENNIS4
216.81.94.73	50.232.155.146	57407	443	6	8	1303	FS PA	2016/02/28T08:20:48.049	78.575	2016/02/28T08:22:06.624	STENNIS4
216.81.94.73	50.232.155.146	57410	443	6	11	1992	FS PA	2016/02/28T08:20:48.054	78.57	2016/02/28T08:22:06.624	STENNIS4
216.81.94.73	50.232.155.146	57412	443	6	9	1371	FS PA	2016/02/28T08:20:48.055	78.568	2016/02/28T08:22:06.623	STENNIS4
216.81.94.73	50.232.155.146	57411	443	6	11	1992	FS PA	2016/02/28T08:20:48.055	78.568	2016/02/28T08:22:06.623	STENNIS4
50.232.155.146	216.81.94.73	443	57409	6	6	2618	FS PA	2016/02/28T08:20:48.104	78.519	2016/02/28T08:22:06.623	STENNIS4
50.232.155.146	216.81.94.73	443	57408	6	9	6395	FS PA	2016/02/28T08:20:48.104	78.52	2016/02/28T08:22:06.624	STENNIS4
50.232.155.146	216.81.94.73	443	57406	6	16	16311	FS PA	2016/02/28T08:20:48.104	78.52	2016/02/28T08:22:06.624	STENNIS4
50.232.155.146	216.81.94.73	443	57407	6	6	2522	FS PA	2016/02/28T08:20:48.104	78.52	2016/02/28T08:22:06.624	STENNIS4
50.232.155.146	216.81.94.73	443	57412	6	5	854	FS PA	2016/02/28T08:20:48.109	78.514	2016/02/28T08:22:06.623	STENNIS4
50.232.155.146	216.81.94.73	443	57410	6	8	4631	FS PA	2016/02/28T08:20:48.109	78.515	2016/02/28T08:22:06.624	STENNIS4
50.232.155.146	216.81.94.73	443	57411	6	8	4663	FS PA	2016/02/28T08:20:48.110	78.513	2016/02/28T08:22:06.623	STENNIS4
216.81.81.83	50.232.155.146	1879	443	6	11	1326	FS PA	2016/02/28T08:20:48.585	0.523	2016/02/28T08:20:49.108	DHSCV4
50.232.155.146	216.81.81.83	443	1879	6	8	5935	FS PA	2016/02/28T08:20:48.617	0.491	2016/02/28T08:20:49.108	DHSCV4
216.81.94.73	50.232.155.146	59597	443	6	8	1287	FS PA	2016/02/28T08:22:17.716	98.92	2016/02/28T08:23:56.636	STENNIS4
50.232.155.146	216.81.94.73	443	59597	6	5	870	FS PA	2016/02/28T08:22:17.772	98.864	2016/02/28T08:23:56.636	STENNIS4
216.81.81.83	50.232.155.146	3663	443	6	8	1095	FS PA	2016/02/28T08:22:18.174	0.208	2016/02/28T08:22:18.382	DHSCV4
50.232.155.146	216.81.81.83	443	3663	6	6	1994	FS PA	2016/02/28T08:22:18.206	0.176	2016/02/28T08:22:18.382	DHSCV4
216.81.94.73	50.232.155.145	59603	80	6	16	1724	S PA	2016/02/28T08:22:18.268	131.437	2016/02/28T08:24:29.705	STENNIS4
50.232.155.145	216.81.94.73	80	59603	6	22	28959	SRPA	2016/02/28T08:22:18.323	131.382	2016/02/28T08:24:29.705	STENNIS4
216.81.94.73	50.232.155.145	59612	80	6	15	4196	FSRPA	2016/02/28T08:22:18.524	127.771	2016/02/28T08:24:26.295	STENNIS4
216.81.94.73	50.232.155.145	59613	80	6	65	18094	S PA	2016/02/28T08:22:18.548	266.384	2016/02/28T08:26:44.932	STENNIS4
216.81.94.73	50.232.155.145	59614	80	6	4	1212	S PA	2016/02/28T08:22:18.549	131.155	2016/02/28T08:24:29.704	STENNIS4
50.232.155.145	216.81.94.73	80	59612	6	17	20366	FS PA	2016/02/28T08:22:18.580	127.715	2016/02/28T08:24:26.295	STENNIS4
50.232.155.145	216.81.94.73	80	59614	6	3	1557	SRPA	2016/02/28T08:22:18.603	131.101	2016/02/28T08:24:29.704	STENNIS4
50.232.155.145	216.81.94.73	80	59613	6	77	103411	SRPA	2016/02/28T08:22:18.604	266.328	2016/02/28T08:26:44.932	STENNIS4
216.81.94.73	50.232.155.146	8158	443	6	12	1463	FS PA	2016/02/28T08:32:40.466	116.077	2016/02/28T08:34:36.543	STENNIS4
50.232.155.146	216.81.94.73	443	8158	6	12	11346	FS PA	2016/02/28T08:32:40.522	116.021	2016/02/28T08:34:36.543	STENNIS4
216.81.94.73	50.232.155.133	8505	80	6	6	2749	S PA	2016/02/28T08:32:49.339	131.068	2016/02/28T08:35:00.407	STENNIS4
50.232.155.133	216.81.94.73	80	8505	6	4	946	SRPA	2016/02/28T08:32:49.395	131.012	2016/02/28T08:35:00.407	STENNIS4
216.81.94.73	50.232.155.130	8592	443	6	43	3711	FS PA	2016/02/28T08:32:53.519	103.024	2016/02/28T08:34:36.543	STENNIS4
50.232.155.130	216.81.94.73	443	8592	6	58	81279	FS PA	2016/02/28T08:32:53.577	102.966	2016/02/28T08:34:36.543	STENNIS4
216.81.94.73	50.232.155.130	8614	443	6	16	2168	FS PA	2016/02/28T08:32:54.585	101.957	2016/02/28T08:34:36.542	STENNIS4
216.81.94.73	50.232.155.130	8613	443	6	8	1230	FS PA	2016/02/28T08:32:54.585	101.957	2016/02/28T08:34:36.542	STENNIS4
216.81.94.73	50.232.155.130	8615	443	6	8	1230	FS PA	2016/02/28T08:32:54.590	101.953	2016/02/28T08:34:36.543	STENNIS4
216.81.94.73	50.232.155.130	8616	443	6	11	1908	FS PA	2016/02/28T08:32:54.591	101.952	2016/02/28T08:34:36.543	STENNIS4
216.81.94.73	50.232.155.130	8617	443	6	10	1856	FS PA	2016/02/28T08:32:54.591	101.952	2016/02/28T08:34:36.543	STENNIS4
216.81.94.73	50.232.155.130	8618	443	6	8	1246	FS PA	2016/02/28T08:32:54.592	101.951	2016/02/28T08:34:36.543	STENNIS4
216.81.94.73	50.232.155.130	8620	443	6	11	1908	FS PA	2016/02/28T08:32:54.593	101.95	2016/02/28T08:34:36.543	STENNIS4
216.81.94.73	50.232.155.130	8621	443	6	14	2698	FS PA	2016/02/28T08:32:54.596	126.341	2016/02/28T08:35:00.937	STENNIS4
50.232.155.130	216.81.94.73	443	8613	6	6	2550	FS PA	2016/02/28T08:32:54.640	101.902	2016/02/28T08:34:36.542	STENNIS4
50.232.155.130	216.81.94.73	443	8614	6	16	16227	FS PA	2016/02/28T08:32:54.641	101.901	2016/02/28T08:34:36.542	STENNIS4
50.232.155.130	216.81.94.73	443	8616	6	8	4547	FS PA	2016/02/28T08:32:54.647	101.896	2016/02/28T08:34:36.543	STENNIS4
50.232.155.130	216.81.94.73	443	8615	6	6	2454	FS PA	2016/02/28T08:32:54.647	101.896	2016/02/28T08:34:36.543	STENNIS4
50.232.155.130	216.81.94.73	443	8617	6	8	4563	FS PA	2016/02/28T08:32:54.648	101.895	2016/02/28T08:34:36.543	STENNIS4
50.232.155.130	216.81.94.73	443	8618	6	6	2166	FS PA	2016/02/28T08:32:54.648	101.895	2016/02/28T08:34:36.543	STENNIS4
50.232.155.130	216.81.94.73	443	8620	6	8	4563	FS PA	2016/02/28T08:32:54.649	101.894	2016/02/28T08:34:36.543	STENNIS4
50.232.155.130	216.81.94.73	443	8621	6	10	6944	FS PA	2016/02/28T08:32:54.653	126.284	2016/02/28T08:35:00.937	STENNIS4
216.81.81.83	50.232.155.130	17746	443	6	11	1429	FS PA	2016/02/28T08:32:55.112	114.208	2016/02/28T08:34:49.320	DHSCV4
50.232.155.130	216.81.81.83	443	17746	6	11	10591	FS PA	2016/02/28T08:32:55.147	114.173	2016/02/28T08:34:49.320	DHSCV4
216.81.94.73	50.232.155.130	11578	443	6	17	3488	FS PA	2016/02/28T08:35:01.011	190.396	2016/02/28T08:38:11.407	STENNIS4
50.232.155.130	216.81.94.73	443	11578	6	14	12473	SRPA	2016/02/28T08:35:01.067	190.34	2016/02/28T08:38:11.407	STENNIS4
216.81.94.73	50.232.155.130	12792	443	6	7	1892	S PA	2016/02/28T08:35:45.412	129.914	2016/02/28T08:37:55.326	STENNIS4
216.81.94.73	50.232.155.130	12791	443	6	7	1274	FS PA	2016/02/28T08:35:45.412	145.993	2016/02/28T08:38:11.405	STENNIS4
216.81.94.73	50.232.155.130	12793	443	6	7	1290	FS PA	2016/02/28T08:35:45.412	145.993	2016/02/28T08:38:11.405	STENNIS4
216.81.94.73	50.232.155.130	12790	443	6	8	1960	FS PA	2016/02/28T08:35:45.412	145.993	2016/02/28T08:38:11.405	STENNIS4
216.81.94.73	50.232.155.130	12795	443	6	8	1944	FS PA	2016/02/28T08:35:45.413	145.992	2016/02/28T08:38:11.405	STENNIS4
216.81.94.73	50.232.155.130	12794	443	6	7	1274	FS PA	2016/02/28T08:35:45.413	145.993	2016/02/28T08:38:11.406	STENNIS4
216.81.94.73	50.232.155.130	12796	443	6	8	1944	FS PA	2016/02/28T08:35:45.414	145.991	2016/02/28T08:38:11.405	STENNIS4
216.81.94.73	50.232.155.130	12797	443	6	9	1996	FS PA	2016/02/28T08:35:45.415	145.991	2016/02/28T08:38:11.406	STENNIS4
50.232.155.130	216.81.94.73	443	12791	6	5	662	SRPA	2016/02/28T08:35:45.468	145.937	2016/02/28T08:38:11.405	STENNIS4
50.232.155.130	216.81.94.73	443	12793	6	5	662	SRPA	2016/02/28T08:35:45.468	145.937	2016/02/28T08:38:11.405	STENNIS4
50.232.155.130	216.81.94.73	443	12790	6	6	1007	SRPA	2016/02/28T08:35:45.468	145.937	2016/02/28T08:38:11.405	STENNIS4
50.232.155.130	216.81.94.73	443	12794	6	5	662	SRPA	2016/02/28T08:35:45.468	145.938	2016/02/28T08:38:11.406	STENNIS4
50.232.155.130	216.81.94.73	443	12792	6	6	975	SRPA	2016/02/28T08:35:45.469	129.857	2016/02/28T08:37:55.326	STENNIS4
50.232.155.130	216.81.94.73	443	12796	6	6	975	SRPA	2016/02/28T08:35:45.470	145.935	2016/02/28T08:38:11.405	STENNIS4
50.232.155.130	216.81.94.73	443	12795	6	6	991	SRPA	2016/02/28T08:35:45.470	145.935	2016/02/28T08:38:11.405	STENNIS4
50.232.155.130	216.81.94.73	443	12797	6	6	991	SRPA	2016/02/28T08:35:45.471	145.935	2016/02/28T08:38:11.406	STENNIS4
216.81.94.73	50.232.155.146	13359	443	6	19	2424	FS PA	2016/02/28T08:36:10.587	120.818	2016/02/28T08:38:11.405	STENNIS4
50.232.155.146	216.81.94.73	443	13359	6	20	21751	FS PA	2016/02/28T08:36:10.643	120.762	2016/02/28T08:38:11.405	STENNIS4
216.81.94.73	50.232.155.146	13386	443	6	18	1951	FS PA	2016/02/28T08:36:11.134	120.27	2016/02/28T08:38:11.404	STENNIS4
216.81.94.73	50.232.155.146	13387	443	6	70	10988	FS PA	2016/02/28T08:36:11.134	189.967	2016/02/28T08:39:21.101	STENNIS4
50.232.155.146	216.81.94.73	443	13386	6	20	24055	FS PA	2016/02/28T08:36:11.189	120.215	2016/02/28T08:38:11.404	STENNIS4
50.232.155.146	216.81.94.73	443	13387	6	89	118006	FS PA	2016/02/28T08:36:11.190	189.911	2016/02/28T08:39:21.101	STENNIS4
216.81.94.73	50.232.155.146	17029	443	6	28	4507	FS PA	2016/02/28T08:39:21.179	149.914	2016/02/28T08:41:51.093	STENNIS4
50.232.155.146	216.81.94.73	443	17029	6	35	43751	FS PA	2016/02/28T08:39:21.235	149.858	2016/02/28T08:41:51.093	STENNIS4
216.81.94.73	50.232.155.133	18524	80	6	32	4975	S PA	2016/02/28T08:40:37.397	143.763	2016/02/28T08:43:01.160	STENNIS4
50.232.155.133	216.81.94.73	80	18524	6	44	60232	SRPA	2016/02/28T08:40:37.453	143.707	2016/02/28T08:43:01.160	STENNIS4
216.81.94.73	50.232.155.130	18770	443	6	16	3452	FS PA	2016/02/28T08:40:52.117	68.853	2016/02/28T08:42:00.970	STENNIS4
50.232.155.130	216.81.94.73	443	18770	6	14	11829	FS PA	2016/02/28T08:40:52.174	68.796	2016/02/28T08:42:00.970	STENNIS4
216.81.94.73	50.232.155.130	18811	443	6	11	2718	FS PA	2016/02/28T08:40:52.648	68.323	2016/02/28T08:42:00.971	STENNIS4
216.81.94.73	50.232.155.130	18812	443	6	11	2718	FS PA	2016/02/28T08:40:52.650	68.322	2016/02/28T08:42:00.972	STENNIS4
216.81.94.73	50.232.155.130	18813	443	6	12	2754	FS PA	2016/02/28T08:40:52.652	68.321	2016/02/28T08:42:00.973	STENNIS4
216.81.94.73	50.232.155.130	18814	443	6	20	4230	FS PA	2016/02/28T08:40:52.655	68.307	2016/02/28T08:42:00.962	STENNIS4
216.81.94.73	50.232.155.130	18815	443	6	14	3460	FS PA	2016/02/28T08:40:52.658	68.315	2016/02/28T08:42:00.973	STENNIS4
216.81.94.73	50.232.155.130	18816	443	6	12	2738	FS PA	2016/02/28T08:40:52.659	68.306	2016/02/28T08:42:00.965	STENNIS4
216.81.94.73	50.232.155.130	18817	443	6	12	2738	FS PA	2016/02/28T08:40:52.659	68.31	2016/02/28T08:42:00.969	STENNIS4
216.81.94.73	50.232.155.130	18818	443	6	12	2786	FS PA	2016/02/28T08:40:52.660	68.309	2016/02/28T08:42:00.969	STENNIS4
50.232.155.130	216.81.94.73	443	18811	6	7	1300	FS PA	2016/02/28T08:40:52.704	68.267	2016/02/28T08:42:00.971	STENNIS4

Obtained via FOIA by Judicial Watch, Inc.

50.232.155.130	216.81.94.73	443	18812	6	7	1332	FS PA	2016/02/28T08:40:52.707	68.265	2016/02/28T08:42:00.972	STENNIS4
50.232.155.130	216.81.94.73	443	18813	6	7	1316	FS PA	2016/02/28T08:40:52.709	68.264	2016/02/28T08:42:00.973	STENNIS4
50.232.155.130	216.81.94.73	443	18814	6	15	12462	FS PA	2016/02/28T08:40:52.711	68.251	2016/02/28T08:42:00.962	STENNIS4
50.232.155.130	216.81.94.73	443	18816	6	7	1316	FS PA	2016/02/28T08:40:52.714	68.251	2016/02/28T08:42:00.965	STENNIS4
50.232.155.130	216.81.94.73	443	18815	6	8	1629	FS PA	2016/02/28T08:40:52.714	68.259	2016/02/28T08:42:00.973	STENNIS4
50.232.155.130	216.81.94.73	443	18817	6	7	1300	FS PA	2016/02/28T08:40:52.715	68.254	2016/02/28T08:42:00.969	STENNIS4
50.232.155.130	216.81.94.73	443	18818	6	7	1332	FS PA	2016/02/28T08:40:52.716	68.253	2016/02/28T08:42:00.969	STENNIS4
216.81.94.73	50.232.155.133	21320	80	6	37	7684	S PA	2016/02/28T08:43:01.587	149.825	2016/02/28T08:45:31.412	STENNIS4
50.232.155.133	216.81.94.73	80	21320	6	46	60598	SRPA	2016/02/28T08:43:01.645	149.767	2016/02/28T08:45:31.412	STENNIS4
216.81.94.73	50.232.155.146	21535	443	6	15	1646	FS PA	2016/02/28T08:43:12.942	86.278	2016/02/28T08:44:39.220	STENNIS4
50.232.155.146	216.81.94.73	443	21535	6	14	15031	FS PA	2016/02/28T08:43:12.998	86.222	2016/02/28T08:44:39.220	STENNIS4
216.81.94.73	50.232.155.130	21611	443	6	17	3041	FS PA	2016/02/28T08:43:21.237	77.982	2016/02/28T08:44:39.219	STENNIS4
50.232.155.130	216.81.94.73	443	21611	6	15	15481	FS PA	2016/02/28T08:43:21.295	77.924	2016/02/28T08:44:39.219	STENNIS4
216.81.94.73	50.232.155.130	21619	443	6	8	1326	FS PA	2016/02/28T08:43:21.828	77.391	2016/02/28T08:44:39.219	STENNIS4
216.81.94.73	50.232.155.130	21620	443	6	11	2690	SRPA	2016/02/28T08:43:21.828	157.648	2016/02/28T08:45:59.476	STENNIS4
216.81.94.73	50.232.155.130	21621	443	6	8	1310	FS PA	2016/02/28T08:43:21.830	77.39	2016/02/28T08:44:39.220	STENNIS4
50.232.155.130	216.81.94.73	443	21619	6	5	674	FS PA	2016/02/28T08:43:21.885	77.334	2016/02/28T08:44:39.219	STENNIS4
50.232.155.130	216.81.94.73	443	21620	6	6	1600	S PA	2016/02/28T08:43:21.885	157.591	2016/02/28T08:45:59.476	STENNIS4
50.232.155.130	216.81.94.73	443	21621	6	5	674	FS PA	2016/02/28T08:43:21.886	77.334	2016/02/28T08:44:39.220	STENNIS4
216.81.94.73	50.232.155.130	21626	443	6	10	2016	FS PA	2016/02/28T08:43:22.037	77.182	2016/02/28T08:44:39.219	STENNIS4
216.81.94.73	50.232.155.130	21627	443	6	10	2032	FS PA	2016/02/28T08:43:22.040	77.178	2016/02/28T08:44:39.218	STENNIS4
216.81.94.73	50.232.155.130	21628	443	6	10	2016	FS PA	2016/02/28T08:43:22.042	77.176	2016/02/28T08:44:39.218	STENNIS4
216.81.94.73	50.232.155.130	21629	443	6	10	2032	FS PA	2016/02/28T08:43:22.042	77.177	2016/02/28T08:44:39.219	STENNIS4
50.232.155.130	216.81.94.73	443	21626	6	6	1003	FS PA	2016/02/28T08:43:22.093	77.126	2016/02/28T08:44:39.219	STENNIS4
50.232.155.130	216.81.94.73	443	21627	6	6	1003	FS PA	2016/02/28T08:43:22.097	77.121	2016/02/28T08:44:39.218	STENNIS4
50.232.155.130	216.81.94.73	443	21628	6	6	1003	FS PA	2016/02/28T08:43:22.098	77.12	2016/02/28T08:44:39.218	STENNIS4
50.232.155.130	216.81.94.73	443	21629	6	6	987	FS PA	2016/02/28T08:43:22.099	77.12	2016/02/28T08:44:39.219	STENNIS4
216.81.81.82	50.232.155.133	4139	80	6	5	878	SRPA	2016/02/28T19:19:16.740	0.183	2016/02/28T19:19:16.923	DHSCV4
50.232.155.133	216.81.81.82	80	4139	6	3	870	S PA	2016/02/28T19:19:16.772	0.151	2016/02/28T19:19:16.923	DHSCV4
216.81.81.82	50.232.155.133	4142	80	6	6	520	FSRPA	2016/02/28T19:19:16.890	0.312	2016/02/28T19:19:17.202	DHSCV4
50.232.155.133	216.81.81.82	80	4142	6	7	9060	S A	2016/02/28T19:19:16.923	0.279	2016/02/28T19:19:17.202	DHSCV4
216.81.81.82	50.232.155.133	4155	80	6	59	3803	SRPA	2016/02/28T19:19:17.167	1.201	2016/02/28T19:19:18.368	DHSCV4
50.232.155.133	216.81.81.82	80	4155	6	81	118683	S PA	2016/02/28T19:19:17.200	1.168	2016/02/28T19:19:18.368	DHSCV4
216.81.81.82	50.232.155.133	4333	80	6	5	601	FS PA	2016/02/28T19:19:18.335	0.103	2016/02/28T19:19:18.438	DHSCV4
50.232.155.133	216.81.81.82	80	4333	6	3	257	FS PA	2016/02/28T19:19:18.368	0.07	2016/02/28T19:19:18.438	DHSCV4
216.81.81.82	50.232.155.133	4339	80	6	5	600	FS PA	2016/02/28T19:19:18.476	0.099	2016/02/28T19:19:18.575	DHSCV4
216.81.81.82	50.232.155.133	4340	80	6	5	600	FS PA	2016/02/28T19:19:18.480	0.1	2016/02/28T19:19:18.580	DHSCV4
216.81.81.82	50.232.155.133	4341	80	6	5	602	FS PA	2016/02/28T19:19:18.484	0.101	2016/02/28T19:19:18.585	DHSCV4
50.232.155.133	216.81.81.82	80	4339	6	3	257	FS PA	2016/02/28T19:19:18.508	0.067	2016/02/28T19:19:18.575	DHSCV4
50.232.155.133	216.81.81.82	80	4340	6	3	256	FS PA	2016/02/28T19:19:18.512	0.068	2016/02/28T19:19:18.580	DHSCV4
50.232.155.133	216.81.81.82	80	4341	6	3	257	FS PA	2016/02/28T19:19:18.517	0.068	2016/02/28T19:19:18.585	DHSCV4
216.81.81.82	50.232.155.133	4352	80	6	6	2324	S PA	2016/02/28T19:19:18.689	128.269	2016/02/28T19:21:26.958	DHSCV4
50.232.155.133	216.81.81.82	80	4352	6	4	667	SRPA	2016/02/28T19:19:18.722	128.236	2016/02/28T19:21:26.958	DHSCV4
216.81.81.82	50.232.155.133	42719	80	6	5	604	FS PA	2016/02/28T19:29:08.194	0.1	2016/02/28T19:29:08.294	DHSCV4
50.232.155.133	216.81.81.82	80	42719	6	3	256	FS PA	2016/02/28T19:29:08.226	0.068	2016/02/28T19:29:08.294	DHSCV4
216.81.81.82	50.232.155.133	43233	80	6	14	2609	SRPA	2016/02/28T19:29:16.717	0.507	2016/02/28T19:29:17.224	DHSCV4
50.232.155.133	216.81.81.82	80	43233	6	14	17663	S PA	2016/02/28T19:29:16.750	0.474	2016/02/28T19:29:17.224	DHSCV4
216.81.81.82	50.232.155.133	43263	80	6	5	601	FS PA	2016/02/28T19:29:17.134	0.101	2016/02/28T19:29:17.235	DHSCV4
216.81.81.82	50.232.155.133	43265	80	6	5	594	FS PA	2016/02/28T19:29:17.140	0.1	2016/02/28T19:29:17.240	DHSCV4
50.232.155.133	216.81.81.82	80	43263	6	3	257	FS PA	2016/02/28T19:29:17.167	0.068	2016/02/28T19:29:17.235	DHSCV4
50.232.155.133	216.81.81.82	80	43265	6	3	257	FS PA	2016/02/28T19:29:17.173	0.067	2016/02/28T19:29:17.240	DHSCV4
216.81.81.82	50.232.155.133	43277	80	6	5	598	FS PA	2016/02/28T19:29:17.191	0.101	2016/02/28T19:29:17.292	DHSCV4
50.232.155.133	216.81.81.82	80	43277	6	3	256	FS PA	2016/02/28T19:29:17.224	0.068	2016/02/28T19:29:17.292	DHSCV4
216.81.81.82	50.232.155.133	43289	80	6	4	1488	S PA	2016/02/28T19:29:17.247	130.666	2016/02/28T19:31:27.913	DHSCV4
216.81.81.82	50.232.155.133	43291	80	6	10	2931	S PA	2016/02/28T19:29:17.258	140.671	2016/02/28T19:31:37.929	DHSCV4
50.232.155.133	216.81.81.82	80	43289	6	3	404	SRPA	2016/02/28T19:29:17.279	130.634	2016/02/28T19:31:27.913	DHSCV4
50.232.155.133	216.81.81.82	80	43291	6	11	11784	SRPA	2016/02/28T19:29:17.290	140.639	2016/02/28T19:31:37.929	DHSCV4
216.81.81.82	50.232.155.133	57181	80	6	4	1573	S PA	2016/02/28T19:33:01.907	131.361	2016/02/28T19:35:13.268	DHSCV4
50.232.155.133	216.81.81.82	80	57181	6	3	404	SRPA	2016/02/28T19:33:01.940	131.328	2016/02/28T19:35:13.268	DHSCV4
216.81.81.82	50.232.155.133	57185	80	6	4	1573	S PA	2016/02/28T19:33:01.941	131.326	2016/02/28T19:35:13.267	DHSCV4
50.232.155.133	216.81.81.82	80	57185	6	3	404	SRPA	2016/02/28T19:33:01.973	131.294	2016/02/28T19:35:13.267	DHSCV4
216.81.81.82	50.232.155.133	41475	80	6	4	1418	S PA	2016/02/28T19:45:11.394	133.074	2016/02/28T19:47:24.468	DHSCV4
50.232.155.133	216.81.81.82	80	41475	6	3	404	SRPA	2016/02/28T19:45:11.425	133.043	2016/02/28T19:47:24.468	DHSCV4

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
To:	"/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"
CC:	"/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"; (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Subject:	RE: Log file - SEN Number 2016-12-093
Date:	2016/12/12 16:22:48
Priority:	Normal
Type:	Note

(b)(6)

Please initiate a packet capture as discussed using the OOB, details to compare can be found in SEN Number 2016-12-093.

Georgia Website http://sos.ga.gov/

MLo Site for License search http://verify.sos.ga.gov/verification/

License information below can be used to test the traffic. You can see how pulling a document from MLo works

(b)(6)

(b)(6)

Please document your findings, and report back.

v/r
(b)(6) (b)(6)
Information Security Analyst
General Dynamics Information Technology



cid:image001.png@01D172C8.F2C16000

From: (b)(6) (b)(
Sent: Monday, December 12, 2016 2:38 PM
To: DHS ESOC Analysts <(b)(6)>
Cc: DHS ESOC Leads <(b)(6)>
Subject: FW: Log file

ALCON –

Obtained via FOIA by Judicial Watch, Inc.

To help with testing, see the below information. Perhaps we can wireshark some of this and see if something blows up.

(b)((b)(6)
(Acting) Chief, DHS ESOC
Office of the Chief Information Security Officer
Department of Homeland Security
Mobile: 202-657-(b)(6)

From: Beaver, Merritt [mailto:(b)(6)
Sent: Monday, December 12, 2016 2:34 PM
To: (b)(6) (b)((b)(6)
Subject: RE: Log file

Here a couple of licenses that have attached documents. You can see how pulling a document from MLo works

(b)(6)

(b)(6)

(b)(6)
Chief Information Officer
Office of Georgia Secretary of State Brian P. Kemp
Office (404) 656-(b)(6) Mobile: (770)330-(b)(6)
(b)(6)

From: (b)(6) (b)((b)(6)
Sent: Monday, December 12, 2016 1:50 PM
To: Beaver, Merritt <(b)(6)>
Subject: RE: Log file

Thank you sir. We're processing it now.

(b)((b)(6)
(Acting) Chief, DHS ESOC
Office of the Chief Information Security Officer
Department of Homeland Security
Mobile: 202-657-(b)(6)

From: Beaver, Merritt (b)(6)
Sent: Monday, December 12, 2016 1:42 PM
To: (b)(6) (b)((b)(6)
Subject: Log file

Georgia Website http://sos.ga.gov/

MLo Site for License search http://verify.sos.ga.gov/verification/

Obtained via FOIA by Judicial Watch, Inc.

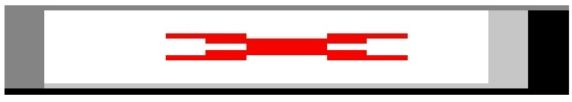
Merritt

S. Merritt Beaver
Chief Information Officer
Office of Georgia Secretary of State Brian P. Kemp
2 Martin Luther King Jr. Drive
(b)(6), West Tower
Atlanta, GA 30334
Office (404) 656-(b)(6) Mobile: (770)330-(b)(6)
(b)(6)

Sender:	(b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Recipient:	"/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"; (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Sent Date:	2016/12/12 16:22:46
Delivered Date:	2016/12/12 16:22:48
From:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
To:	(b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
CC:	(b)(6) (b)(6 </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Subject:	Georgia logs
Date:	2016/12/12 14:45:36
Priority:	Normal
Type:	Note

Hey guys,

As I'm getting ready to leave for the day, let me share with you what I've noticed so far.



This report is for events containing source IP 216.81.81[.]80 **OR** destination IP 50.232.155[.]145.
Therefore there is only one event that concerns us. (page 2)

Ticket Detail: (page92)

Obtained via FOIA by Judicial Watch, Inc.

32493075 2016 -11-15 13:43:25 1 216 .81.81.80 50.232.155.14 5 Not Blocked HTTP OPTIONS Method

Event Detail: (page 95)
Nov 15 08:43:23 10.1.0.2 1,2016 /11/15
08:43:22,001801015967 ,THREAT,vulnerability,1,2016 /11/15
08:43:22,216.81.81.80 ,50.232.155.145,216.81.81.80 ,10.250.0.10,inboundweb-
bro wsing,,,web-browsing,vsys1,o utside,dmz,ethernet1/4,ether net1/2,dellsecureworks,
2016 /11/15 08:43:22,247985,1,636 36,80,63636,80,0x402000,tcp,
alert,"",HTTP OPTIONS Method (30520),government,informational,client-to-server,500430
600,0x0,US,US,0,,0,,,1,,,,,, ,,0,0,0,0,0,,ATL-PAN-01,

Incident Overview of note:

"The CTOC has received an alert for 'HTTP OPTIONS Method' from your Palo Al to FW device (10.1.0.2/firewall01) for traffic (Not Bloc ked) sourcing from port 63636/tcp of 216.81.81.80 (Arlington, USA) destined to port 80/tcp of 50.232.155.145 (Feasterville Trevose, USA) that occurred on 2016-11-15 at 08:43:22. These alerts are indicative of possible vulnerability scanning activity." **(page 93)**

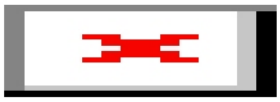
- The cyber security company is reported this event as possible vuln Scanning activity.

".....please verify that Department of Homeland Security is an authorized vulnerability scanning vendor for your company and determine whether the current scanning activity is legitimate. We are escalating this incident to you via a medium priority ticket and no phone call per our default handling policy."

Ticket was escalated (page 95)
15, Nov 2016 08:54:58 **automation Escalation Note**
Escalation Notes were change d on 01/08/2016 01:51:29 PM
SUMMARY OF THOSE CHANGES:
Added 'Possible PHP-CGI String Parsing Vulnerability Exploit Attempts - Ticket Only'

My conclusion – possible misinterpretation of the security event and got escalated up too quickly. Please continue reviewing the report.

v/r
(b)(6) (b)(6) GCIH, Sec+
Security Analyst, SOC – Shift Lead
General Dynamics Information Technology
Enterprise **S**ecurity **O**perations **C**enter (ESOC)
Department of Homeland Security
MGMT/OCIO/OCISO



dhs_esoc_2_info

Sender:	(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Recipient:	(b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP

Obtained via FOIA by Judicial Watch, Inc.

	(b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Sent Date:	2016/12/12 14:45:35
Delivered Date:	2016/12/12 14:45:36

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
To:	"Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
CC:	"Lilly, Tamara </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Tamara.lilly>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Subject:	RE: Recap of Georgia Inquiry Call
Date:	2016/12/09 08:26:02
Priority:	Normal
Type:	Note

Hunh, that complicates things, doesn't it? I'll wait to hear from your folks analysis.

Thanks,

(b)(6)
Director, National Security Systems
Office of the Chief Information Security Officer
Department of Homeland Security
(b)(6)
202-233-(b)(6)

From: Rohner, Boyden
Sent: Friday, December 9, 2016 8:20 AM
To: Dister, Daniel (b)(6) (b)(6)
Cc: Lilly, Tamara (b)(6) Carroll, (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (CTR) (b)(6) (b)(6) (b)((b)(6)
Subject: RE: Recap of Georgia Inquiry Call

Good morning, (b)(6)-

The IP resolved to one of our blue coat proxies - so we don't have a machine identified to pull.

(b)(6) (b)(6) or (b)(6) can elaborate if I've over simplified the explanation.

Obtained via FOIA by Judicial Watch, Inc.

From: (b)(6)
Sent: Friday, December 09, 2016 12:59:08 PM
To: Rohner, Boyden; (b)(6) (b)(6)
Cc: Lilly, Tamara; (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (CTR)
Subject: RE: Recap of Georgia Inquiry Call

Just to offer some advice based on past incidents I have been involved in – since an originating IP was identified, have we (DHS/CBP/DC1) tracked down the machine and pulled it from the network? Locating the offending machine, isolating it from the network and doing a forensic analysis should be a high priority. One benefit of pursuing this approach quickly is that maybe we can't find any such machine using that IP within DHS, and then we can work along the lines that it was a spoofed IP that scanned the State of Georgia.

Just a thought…

(b)(6) CISSP
Director, National Security Systems
Office of the Chief Information Security Officer
Department of Homeland Security
(b)(6)
202-233-(b)(6)

From: Rohner, Boyden
Sent: Thursday, December 8, 2016 5:44 PM
To: (b)(6) (b)(6) (b)(6)
Cc: Lilly, Tamara (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (CTR) (b)(6)
Subject: Recap of Georgia Inquiry Call

Good evening,

- ESOC will make copy of +/-24 hours around 15 Nov and store for later review.
- (b)((b)(6) Acting ESOC Chief will be the primary point of contact for DHS ESOC for anticipated SOC-to-SOC exchange.
- NPPD/IGA will broker the SOC-to-SOC exchange. NPPD will work with OPA on the media points. CIO and CISO may be asked to clear.
- Info needed to aid DHS in our investigation:
  - Addresses of the targets.
  - What were the targeted systems?
  - Logs from the Managed Service Provider for the targeted systems to include source and destination IPs.
  - How large/how many attempts were made and what was the timeframe?
  - Which firewalls (DMZ, internal, etc.) detected the attempts?
  - What ports and protocols were involved?
  - Was 281.81.81.80 the only source observed?
  - What indicators identified this as a scan?

Obtained via FOIA by Judicial Watch, Inc.

- Technical Point of Contact from the MSP, who can facilitate information sharing.

Sender:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
Recipient:	"Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Lilly, Tamara </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Tamara.lilly>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Sent Date:	2016/12/09 08:26:01
Delivered Date:	2016/12/09 08:26:02

Obtained via FOIA by Judicial Watch, Inc.

From:	/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=CSIRC.CBP.DHS.GOV374
To:	(b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"
CC:	"CSIRC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) "; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)
Subject:	RE: Regarding "Letter to Secretary Johnson"
Date:	2016/12/08 21:01:40
Priority:	Normal
Type:	Note

(b)(6

I really appreciate prompt resonse sir. Are you able to provide any context around the “Princess Cruise Lines” traffic referenced in the email below? We thoroughly reviewed bluecoat logs and could not attribute a CBP to both Princess Cruise Lines and the GA SOS site.

What is the “assessment” that ESOC made referenced below regarding the observed “Princess Cruise Lines” reported in the last couple weeks? Or was this statement made in error?

Thank you,

(b)(6)
Cyber Security Operations Center (CSOC)
Cyber Security Directorate (CSD)
Office of Information and Technology (OIT)
Enterprise Services (ES)
U.S. Customs And Border Protection (CBP)
Office: 571468(b)(6) | Mobile: 202738(b)(6)
Email:(b)(6)
CSIRC:(b)(6)

From: (b)(6) (b)(
Sent: Thursday, December 08, 2016 8:48 PM
To:(b)(6) DHS ESOC (b)(6) DHS ESOC Leads (b)(6)
Cc: CSIRC (b)(6) (b)(6)
Subject: RE: Regarding "Letter to Secretary Johnson"

(b)(6) --

Obtained via FOIA by Judicial Watch, Inc.

Glad to have you back in the mix. In point of fact, the IP address in question (81.80) is not CBP, but rather one of the external addresses for general outbound TIC traffic (round-robined from any of the components) . The confusion about this originated from the NCATS team, who associated it with your component (falsely) through their cyber hygiene activities. We have clarified this with NPPD management, OCIO and representatives of the NCATS team at the 1700 touchpoint today, and I will send a follow up email to them (the NCATS team) tomorrow explaining the architecture of the external facing TIC space.

Let me know if you need any additional information.

(b)(6) (b)(6)
(Acting) Chief, DHS ESOC
Office of the Chief Information Security Officer
Department of Homeland Security
Mobile: 202-657-(b)(6)

From: (b)(6)
Sent: Thursday, December 08, 2016 8:19:24 PM
To: DHS ESOC; DHS ESOC Leads
Cc: CSIRC; (b)(6)
Subject: Regarding "Letter to Secretary Johnson"

Good Evening ESOC,

I have to provide our AC with an update on this by NLT 0700. I've been informed by my leadership that there was some email traffic circulating on this topic:

"Sent: Thursday, December 8, 2016 4:53 PM
Subject: RE: Conference call regarding "Letter to Sec. Johnson

As I understand it, the facts as we know it are:

- **This same CBP IP address previously was reported to us by Princess Cruise Lines in the last few weeks. CIO/ESOC assessed that the CBP computer was just doing normal web browsing to Princess Cruise Lines.**
- **ESOC assesses that the CBP computer was just doing normal browsing to Georgia's Secretary of State office on Nov 15 as well."**

CBP CSOC respectfully requests some clarification on the following information:

- Please define "normal browsing" as it is refenced in the text highlighted above.
- How was ESOC able to link that to IP address to CBP when it was reported by Princess Cruise Lines?
- How was ESOC able to assess that the CBP computer was just doing normal browsing activity to Princess Cruise Lines?

Obtained via FOIA by Judicial Watch, Inc.

- Who was the CBP user in this case? And exactly, what Princess Cruise Lines site (dest ip or URL) was this referring to?
- Was CBP notified of the information that Princess Cruise Lines reported?
- How did ESOC link this CBP user to both "Princess Cruise Lines" and the GA SOS Office site on Nov 15th based on the 216.81.81.80 IP? (i.e. who is this user?, what logs do you have to support this claim?)
- In both instances, who made this assessment that all this activity was just "normal browsing"?

This topic is generating a lot of attention from our senior management and we would appreciate a response as soon as possible.

Thank you,

(b)(6)
Cyber Security Operations Center (CSOC)
Cyber Security Directorate (CSD)
Office of Information and Technology (OIT)
Enterprise Services (ES)
U.S. Customs And Border Protection (CBP)
Office: 571468(b)(6) | Mobile: 202738(b)(6)
(b)(6)

Sender:	/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=CSIRC.CBP.DHS.GOV374
Recipient:	(b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Leads4ef"; "CSIRC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN(b)(6) "; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) >"
Sent Date:	2016/12/08 21:01:39
Delivered Date:	2016/12/08 21:01:40

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
To:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
CC:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"
Subject:	RE: Update State of Georgia
Date:	2016/12/14 04:39:33
Priority:	Normal
Type:	Note

Just FYI: I have created an Arcsight channel to monitor for traffic with UA “Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; Tablet PC 2.0; C15IE72011A; ms-office)” and will reach out to ICE/CIS and attempt to identify the PID (application involved) based on the Source port of the traffic.

V/r,
(b)(6)

From: (b)(6) (b)(6) (CTR)
Sent: Wednesday, December 14, 2016 4:17 AM
To: (b)(6) (b)(6) (CTR) (b)(6) (b)(6) (b)(6) (b)(6)
Rohner, Boyden (b)(6) (b)(6) (b)(6) (b)(6)
(b)(6) (b)((b)(6)
Cc: (b)(6) (b)(6) (CTR) (b)(6) DHS ESOC Analysts
(b)(6)
Subject: RE: Update State of Georgia

(b)(6)

In order to identify the HTTP headers, we need the packet capture to check if the requests’ headers are the same on all these OPTIONS requests and unfortunately our pcap retention does not go that far.

In reference to office being the root cause of the traffic, I have noticed that the HTTP OPTIONS request does always precede an actual GET request to the same resource or to a resource in the same folder as the OPTIONS request and that the user Agent for the GET is either “Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E; InfoPath.3; Tablet PC 2.0; IE8Mercury; ms-office) à (Office 2010)” OR “Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR

Obtained via FOIA by Judicial Watch, Inc.

3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 15)à (office 2013)". In order to confirm the hypothesis; I have pulled multiple proxy log samples (unrelated to SEN 2016-12-093) of traffic where User Agent string =" Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; Tablet PC 2.0; C15IE72011A; ms-office)" and sure enough there was an OPTIONS request made right before the GET. The other fact is that this UA is only seeing in ICE/CIS Network and based on my phone conversation with their SOC, they have stated that they do use tablet-PC and have office 2010.

We are still working on identifying what and how is the traffic generated with UA "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; Tablet PC 2.0; C15IE72011A; ms-office)" which would then explain the HTTP OPTIONS requests.





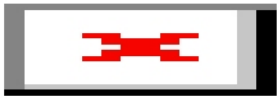


Please let me know if you need more clarifications.

V/r,

(b)(6) (b)(6) GCIA, CNDA/CEH, CCNA Sec
Information Security Analyst
Critical Solutions Inc
Supporting the Enterprise Security Operations Center (ESOC)
Department of Homeland Security
MGMT/OCIO/CISO/SOC
DHS SOC COOP: (540) 542-(b)(6)

Obtained via FOIA by Judicial Watch, Inc.



dhs_esoc_2_info

From: (b)(6) (b)(6) (CTR)
Sent: Tuesday, December 13, 2016 11:38 PM
To: (b)(6) (b)(6) (CTR) (b)(6) (b)(6) (b)(6) (b)(6) Rohner, Boyden (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)((b)(6)
Cc: (b)(6) (b)(6) (CTR) (b)(6) DHS ESOC Analysts (b)(6)
Subject: RE: Update State of Georgia

Also, can we validate that each event involved opening a document on the Web site.
Thanks again -K

From: (b)(6) (b)(6) (CTR)
Sent: Tuesday, December 13, 2016 11:34:49 PM
To: (b)(6) (b)(6) Rohner, Boyden; (b)(6) (b)(6) (b)(6) (b)(
Cc: (b)(6) (b)(6) (CTR); DHS ESOC Analysts
Subject: RE: Update State of Georgia

(b)(6)
One additional data point would help. Can we get what versions of MS Office were on the clients. I have been researching the OPTIONS command and having the Office version, especially in research on how the command is used.
Thanks (b)(6)

From: (b)(6) (b)(6
Sent: Tuesday, December 13, 2016 10:51:31 PM
To: Rohner, Boyden; (b)(6) (b)(6) (b)(6) (b)(
Cc: (b)(6) (b)(6) (CTR); DHS ESOC Analysts; (b)(6) (b)(6) (CTR)
Subject: Update State of Georgia

Good Evening Team,

From our most recent analysis, the new scanning events outlined in the GASOS letter appears to be additional "OPTIONS" request methods coming from the DHS IP space. We currently have splunk web logs showing these events from the Sep 12th event on. The events are as follows:

September 12, 2016 12:52:32 EDT (11:52 CDT)
Host **10.61.22.222** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.georgia.gov/ (Denied)

Obtained via FOIA by Judicial Watch, Inc.

September 28, 2016 08:54:15 EDT (07:54 CDT)
Host **10.56.189.94** (ICE-CIS) attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://sos.ga.gov/index.php/licensing/plb/ (Denied)

October 3, 2016 11:41:32 EDT (10:41 CDT)
Host **10.101.194.178** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.state.ga.us/corporations/ (Denied)

October 6, 2016 11:14:16 EDT (10:14 CDT)
Host **10.32.82.42** (FEMA)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://verify.sos.ga.gov/verification/stylesheets/ (Observed)

November 7, 2016 13:15:43 EST (12:15 CST)
Host **10.56.189.65** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.georgia.gov/plb/cosmetology/ (Denied)

November 8, 2016 08:35:21 EST (07:35 CST)
Host **10.243.15.188** (FLETC)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://verify.sos.ga.gov/verification/stylesheets/ (Observed)

Unfortunately, our Splunk data does not go back as far as February and May. In addition our Einstein Data is not yielding any results (b)(6) is still working it). We have asked all the major components to check their logs for OPTIONS requests going to any GA websites on the remaining "Scan" dates in February and (b)(6) and the night shift will call all the SOCs to ensure they received the message).

Even if they do not yield any results, our other results fit a distinct and precise pattern of traffic. It would be very hard for them to repudiate the findings as anything other than non-malicious Microsoft OPTIONS requests. We will update and brief the Components again at 0900 tomorrow.

I will be following up with the Microsoft team shortly to try and expedite a response on their behalf.

Please feel free to add any additional findings or comments to this thread.

Respectfully,

(b)(6) (b)(6)

Sender:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Recipient:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)

Obtained via FOIA by Judicial Watch, Inc.

	(b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"
Sent Date:	2016/12/14 04:39:32
Delivered Date:	2016/12/14 04:39:33

End Time ↑ 1	Name	Attacker Addre	Attacker P	Target Address	Target Po	Device Action	Request Me	Request Url	Request Client Application	B
13 Dec 2016 18:15:52 EST	TCP_HIT	10.61.234.76	0	34.193.87.113	80	OBSERVED	GET	http://www.americanhighschool.org:80/	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; C15IE72011A; rv:11.0) like Gecko	
13 Dec 2016 18:15:51 EST	TCP_MISS	10.61.234.76	27115	34.193.87.113	80	OBSERVED	GET	http://www.americanhighschool.org:80/	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; Tablet PC 2.0; C15IE72011A; ms-office)	
13 Dec 2016 18:15:49 EST	TCP_DENIED	10.61.234.76	27019	34.193.87.113	80	DENIED	OPTIONS	http://www.americanhighschool.org:80/	Microsoft Office Protocol Discovery	

Obtained via FOIA by Judicial Watch, Inc.

Time	Name	Attacker Addr	Attacker P	Target Addres	Targ	Device Action	Request M	Request Url	Request Client Application
ec 2016 16:34:28 EST	TCP_DENIED	10.61.19.67	46355	192.0.72.26	80	DENIED	OPTIONS	http://liftedlamp.files.wordpress.com:80/2013/07/	Microsoft Office Protocol Discovery
ec 2016 16:34:28 EST	TCP_MISS	10.61.19.67	46479	192.0.72.26	80	OBSERVED	GET	http://liftedlamp.files.wordpress.com:80/2013/07/dhs_cis_wr_at.jpg	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; Tablet PC 2.0; C15IE72011A; ms-office)

Obtained via FOIA by Judicial Watch, Inc.

Time	1	Attacker Address	Attac	Target Address	Targ	Request M	Device Ac	Request Url	Request User Agent
3 Dec 2016 07:38:04 EST		10.179.242.188	52...	107.170.249.167	80	OPTIONS	PROXIED	http://travel.state.gov:80/content/visas/english/fees/	Microsoft Office Protocol Discovery
3 Dec 2016 07:38:04 EST		10.179.242.188	0	107.170.249.167	80	GET	PROXIED	http://travel.state.gov:80/content/visas/english/fees/reciprocity-by-country....	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; Tablet PC 2.0; C15IE72011A; ms-office)

Obtained via FOIA by Judicial Watch, Inc.

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
To:	(b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Tran, (b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6 (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
CC:	(b)(6) (b)(6 (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6 (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6 </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Subject:	RE: Update State of Georgia - SEN 2016-12-093
Date:	2016/12/14 06:51:07
Priority:	Normal
Type:	Note

(b)(6)

Please continue working this SEN to include following up with the components on their searches, and reviewing logs they provided (attached to SEN). Below is what was done this evening, as well as current updates from the components on their searches. All emails the past 12 hours regarding Georgia that were in the DHS ESOC inbox have been archived in the proper SEN folder in Outlook.

1. Splunk searches performed September through November 2016 that identified six (6) DHS IPs belonging to FEMA, FLETC, and ICE-CIS matching the timelines exactly

2. Email notification sent to DHS Component SOCs to perform log searches for February 2nd, February 28th and May 23rd to the Georgia site with Destination IP address of either 50.232.155.157 or 50.232.155.145, which resolves to sos.ga.gov or sos.state.ga.us or verify.sos.ga.gov, HTTP Request Method: “OPTIONS”

3. Email notification sent to component SOCs indicating that they have been added to SEN Number 2016-12-093, to complete the request this evening, and update the SEN

4. DHS ESOC follow-up phone call to component SOCs regarding any questions and status of the request

5. Update on the six (6) DHS IPs have been identified as belonging to 1 USCIS, 3 ICE, 1 FEMA, 1 FLETC

Obtained via FOIA by Judicial Watch, Inc.

6. Einstein searches found some Netflow data that matches the date and time for the Feb 2nd and May 23rd events. Traffic is over TCP/80 and is seen going through Stennis4 E1 sensor. Although there was data for Feb 28th, traffic did not match the 13:19 CST time. Einstein results are attached to SEN Number 2016-12-093. Also, in speaking with ESOC Engineering (Lavar) earlier this evening, he could not provide proxy logs for February and May, as Blue Coat data retention on their log server only goes back to November, and that our tools (Splunk) actually retains the data longer.

7. DHS ESOC has further investigated/analyzed the proxy logs and found that in 4 out of the 6 identified web requests, The OPTIONS requests do always precede actual GET requests to the same resource or to a resource in the same folder as the OPTIONS request and that the user Agent for the GET is either "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E; InfoPath.3; Tablet PC 2.0; IE8Mercury; ms-office). DHS ESOC has created an Arcsight channel to track traffic with the indicated User Agent String and will attempt to correlate the Source Port of any real-time traffic with the Process ID (The application that initiated the traffic).

8. Component updates as of 12/14/2016 @6:30 AM:

- ICE - 12/14/2016 @5:59 AM The ICE SOC is currently working on this request and will provide an update shortly
- FEMA - 12/13/2016 11:25 PM The FEMA-SOC acknowledges this event, will follow up with supervisor at 0630 hours on 12/14/2016
- FLETC - 12/14/2016 @5:56 AM DHS ESOC sent an email to TSA SOC to provide a status of this request
- USCIS - 12/14/2016 2:33 AM USCIS Searched the dates specified below for all traffic to the Georgia URL's and IP's. Events were found and attached to SEN's log.
- CBP - 12/14/2016 12:41 AM CBP SOC searched the dates specified below, and did not find any traffic with the OPTIONS method, but found http traffic destined to sos.ga.gov using the GET method
- DC1 - DC1 - 12/14/2016 12:13 AM DC1 SOC has performed searches on 50.232.155.157/ 50.232.155.145 as well the *.ga.us and *.ga.gov domains and received no hits for the dates DHS ESOC has requested. DC1 SOC is continuing our research.
- DC2 - 12/14/2016 02:46 AM DC2 SOC searched the destination IPs in question received in the original email request on the specific dates suggested and found no immediate results. (50.232.155.157, 50.232.155.145; February 2nd, February 28th and May 23rd, 2016)
- DHSHQ - 12/14/2016 03:32 AM HQ SOC has identified no traffic to the specified IP addresses or URLs for the dates in question. Continuing investigation
- TSA - 12/14/2016 @5:57 AM There were no outgoing / incoming web traffic to the IPs or hostnames mentioned in this SEN.

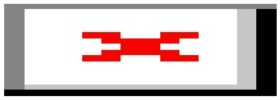
V/r,

(b)(6) (b)(6)

Shift lead, SOC – Incident Handling

Obtained via FOIA by Judicial Watch, Inc.

General Dynamics Information Technology (GDIT)
Supporting the Department of Homeland Security (DHS)
DHS Enterprise Security Operations Center (ESOC)
MGMT/OCIO/CISO/ESOC



dhs_esoc_2_info

From: (b)(6) (b)(6) (CTR)
Sent: Wednesday, December 14, 2016 4:40 AM
To: (b)(6) (b)(6) (CTR) (b)(6) (b)(6) (b)(6) (b)(6)
Rohner, Boyden (b)(6) (b)(6) (b)(6) (b)(6)
(b)(6) (b)((b)(6)
Cc: (b)(6) (b)(6) (CTR) (b)(6) DHS ESOC Analysts
(b)(6)
Subject: RE: Update State of Georgia

Just FYI: I have created an Arcsight channel to monitor for traffic with UA "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; Tablet PC 2.0; C15IE72011A; ms-office)" and will reach out to ICE/CIS and attempt to identify the PID (application involved) based on the Source port of the traffic.

V/r,
(b)(6)

From: (b)(6) (b)(6) (CTR)
Sent: Wednesday, December 14, 2016 4:17 AM
To: (b)(6) (b)(6) (CTR) (b)(6) (b)(6) (b)(6) (b)(6)
Rohner, Boyden (b)(6) (b)(6) (b)(6) (b)(6)
(b)(6) (b)((b)(6)
Cc: (b)(6) (b)(6) (CTR) (b)(6) DHS ESOC Analysts
(b)(6)
Subject: RE: Update State of Georgia

(b)(6)

In order to identify the HTTP headers, we need the packet capture to check if the requests' headers are the same on all these OPTIONS requests and unfortunately our pcap retention does not go that far.

In reference to office being the root cause of the traffic, I have noticed that the HTTP OPTIONS request does always precede an actual GET request to the same resource or to a resource in the same folder as the OPTIONS request and that the user Agent for the GET is either "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E; InfoPath.3; Tablet PC 2.0; IE8Mercury; ms-office) à (Office 2010)" OR "Mozilla/4.0

Obtained via FOIA by Judicial Watch, Inc.

(compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 15)à (office 2013)". In order to confirm the hypothesis; I have pulled multiple proxy log samples (unrelated to SEN 2016-12-093) of traffic where User Agent string =" Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; Tablet PC 2.0; C15IE72011A; ms-office)" and sure enough there was an OPTIONS request made right before the GET. The other fact is that this UA is only seeing in ICE/CIS Network and based on my phone conversation with their SOC, they have stated that they do use tablet-PC and have office 2010.

We are still working on identifying what and how is the traffic generated with UA "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; Tablet PC 2.0; C15IE72011A; ms-office)" which would then explain the HTTP OPTIONS requests.





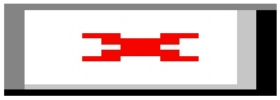


Please let me know if you need more clarifications.

V/r,

(b)(6) (b)(6) GCIA, CNDA/CEH, CCNA Sec
Information Security Analyst
Critical Solutions Inc
Supporting the Enterprise Security Operations Center (ESOC)
Department of Homeland Security
MGMT/OCIO/CISO/SOC
DHS SOC COOP: (540) 542-(b)(6)

Obtained via FOIA by Judicial Watch, Inc.



dhs_esoc_2_info

From: (b)(6) (b)(6) (CTR)
Sent: Tuesday, December 13, 2016 11:38 PM
To: (b)(6) (b)(6) (CTR) (b)(6) (b)(6) (b)(6) (b)(6)
Rohner, Boyden (b)(6) (b)(6) (b)(6) (b)(6)
(b)(6) (b)((b)(6)
Cc: (b)(6) (b)(6) (CTR) (b)(6) DHS ESOC Analysts
(b)(6)
Subject: RE: Update State of Georgia

Also, can we validate that each event involved opening a document on the Web site.
Thanks again -K

From: (b)(6) (b)(6) (CTR)
Sent: Tuesday, December 13, 2016 11:34:49 PM
To: (b)(6) (b)(6) Rohner, Boyden; (b)(6) (b)(6) (b)(6) (b)(
Cc: (b)(6) (b)(6) (CTR); DHS ESOC Analysts
Subject: RE: Update State of Georgia

(b)(6)
One additional data point would help. Can we get what versions of MS Office were on the clients. I have been researching the OPTIONS command and having the Office version, especially in research on how the command is used.
Thanks (b)(6)

From: (b)(6) (b)(6
Sent: Tuesday, December 13, 2016 10:51:31 PM
To: Rohner, Boyden; (b)(6) (b)(6) (b)(6) (b)(
Cc: (b)(6) (b)(6) (CTR); DHS ESOC Analysts; (b)(6) (b)(6) (CTR)
Subject: Update State of Georgia

Good Evening Team,

From our most recent analysis, the new scanning events outlined in the GASOS letter appears to be additional "OPTIONS" request methods coming from the DHS IP space. We currently have splunk web logs showing these events from the Sep 12th event on. The events are as follows:

September 12, 2016 12:52:32 EDT (11:52 CDT)
Host **10.61.22.222** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.georgia.gov/ (Denied)

Obtained via FOIA by Judicial Watch, Inc.

September 28, 2016 08:54:15 EDT (07:54 CDT)
Host **10.56.189.94** (ICE-CIS) attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://sos.ga.gov/index.php/licensing/plb/ (Denied)

October 3, 2016 11:41:32 EDT (10:41 CDT)
Host **10.101.194.178** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.state.ga.us/corporations/ (Denied)

October 6, 2016 11:14:16 EDT (10:14 CDT)
Host **10.32.82.42** (FEMA)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://verify.sos.ga.gov/verification/stylesheets/ (Observed)

November 7, 2016 13:15:43 EST (12:15 CST)
Host **10.56.189.65** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.georgia.gov/plb/cosmetology/ (Denied)

November 8, 2016 08:35:21 EST (07:35 CST)
Host **10.243.15.188** (FLETC)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://verify.sos.ga.gov/verification/stylesheets/ (Observed)

Unfortunately, our Splunk data does not go back as far as February and May. In addition our Einstein Data is not yielding any results (b)(6) is still working it). We have asked all the major components to check their logs for OPTIONS requests going to any GA websites on the remaining "Scan" dates in February and (b)(6) and the night shift will call all the SOCs to ensure they received the message).

Even if they do not yield any results, our other results fit a distinct and precise pattern of traffic. It would be very hard for them to repudiate the findings as anything other than non-malicious Microsoft OPTIONS requests. We will update and brief the Components again at 0900 tomorrow.

I will be following up with the Microsoft team shortly to try and expedite a response on their behalf.

Please feel free to add any additional findings or comments to this thread.

Respectfully,

(b)(6) (b)(6)

Sender:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Recipient:	(b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (b)((CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6 (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) >";

Obtained via FOIA by Judicial Watch, Inc.

	"/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Sent Date:	2016/12/14 06:51:05
Delivered Date:	2016/12/14 06:51:07

Obtained via FOIA by Judicial Watch, Inc.

From:	Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=BOYDEN.ROHNER>
To:	(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
CC:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Subject:	RE: Update State of Georgia
Date:	2016/12/13 23:04:38
Priority:	Normal
Type:	Note

Thank you all very much.

I'm very impressed and proud of your quick turn around on this tonight.

Sincerely,
Boyden

From: (b)(6) (b)(6)
Sent: Wednesday, December 14, 2016 3:51:31 AM
To: Rohner, Boyden; (b)(6) (b)(6) (b)(6) (b)(
Cc: (b)(6) (b)(6) (CTR); DHS ESOC Analysts; (b)(6) (b)(6) (CTR)
Subject: Update State of Georgia

Good Evening Team,

From our most recent analysis, the new scanning events outlined in the GASOS letter appears to be additional "OPTIONS" request methods coming from the DHS IP space. We currently have splunk web logs showing these events from the Sep 12th event on. The events are as follows:

September 12, 2016 12:52:32 EDT (11:52 CDT)
Host **10.61.22.222** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.georgia.gov/ (Denied)

September 28, 2016 08:54:15 EDT (07:54 CDT)
Host **10.56.189.94** (ICE-CIS) attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://sos.ga.gov/index.php/licensing/plb/ (Denied)

Obtained via FOIA by Judicial Watch, Inc.

October 3, 2016 11:41:32 EDT (10:41 CDT)
Host **10.101.194.178** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.state.ga.us/corporations/ (Denied)

October 6, 2016 11:14:16 EDT (10:14 CDT)
Host **10.32.82.42** (FEMA) attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://verify.sos.ga.gov/verification/stylesheets/ (Observed)

November 7, 2016 13:15:43 EST (12:15 CST)
Host **10.56.189.65** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.georgia.gov/plb/cosmetology/ (Denied)

November 8, 2016 08:35:21 EST (07:35 CST)
Host **10.243.15.188** (FLETC)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://verify.sos.ga.gov/verification/stylesheets/ (Observed)

Unfortunately, our Splunk data does not go back as far as February and May. In addition our Einstein Data is not yielding any results (b)(6) is still working it). We have asked all the major components to check their logs for OPTIONS requests going to any GA websites on the remaining "Scan" dates in February and (b)(6) and the night shift will call all the SOCs to ensure they received the message).

Even if they do not yield any results, our other results fit a distinct and precise pattern of traffic. It would be very hard for them to repudiate the findings as anything other than non-malicious Microsoft OPTIONS requests. We will update and brief the Components again at 0900 tomorrow.

I will be following up with the Microsoft team shortly to try and expedite a response on their behalf.

Please feel free to add any additional findings or comments to this thread.

Respectfully,

(b)(6) (b)(6)

Sender:	Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=BOYDEN.ROHNER>
Recipient:	(b)(6) (b)(6 </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"; (b)(6) (b)(6 (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP

Obtained via FOIA by Judicial Watch, Inc.

	(b)(6)
Sent Date:	2016/12/13 23:04:37
Delivered Date:	2016/12/13 23:04:38

Obtained via FOIA by Judicial Watch, Inc.

From:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
To:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
CC:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"
Subject:	RE: Update State of Georgia
Date:	2016/12/14 07:54:01
Priority:	Normal
Type:	Note

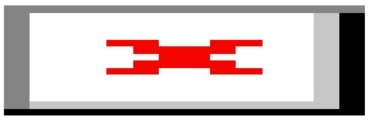
All,
You may already know this but fysa:

The OPTION HTTP method is a default function for the latest bowsers implemented as a security function through CORS (Cross-origin resource sharing). If a request is made with non-standard HTTP headers, the browser will automatically send an OPTION method first to determine if the server will accept the non-standard HTTP headers. CORS is intended to enhance security by minimizing unauthorized cross-site scripting attempts.

https://en.wikipedia.org/wiki/Cross-origin_resource_sharing#Browser_support
https://upload.wikimedia.org/wikipedia/commons/c/ca/Flowchart_showing_Simple_and_Preflight_XHR.svg

R,
(b)(6) (b)(6
Information Security Analyst
General Dynamics Information Technology (GDIT)
Supporting the Department of Homeland Security (DHS)
MGMT/OCIO/CISO/SOC
DHS ESOC Main Line: 1-877-347-(b)(6)
DHS ESOC COOP: (540) 542-(b)(6)

Obtained via FOIA by Judicial Watch, Inc.



cid:image001.png@01D15F3E.16F9DD60

From: (b)(6) (b)(6) (CTR)
Sent: Wednesday, December 14, 2016 4:17 AM
To: (b)(6) (b)(6) (CTR) (b)(6) (b)(6) (b)(6) (b)(6)
Rohner, Boyden (b)(6) (b)(6) (b)(6) (b)(6)
(b)(6) (b)((b)(6)
Cc: (b)(6) (b)(6) (CTR) (b)(6) DHS ESOC Analysts
(b)(6)
Subject: RE: Update State of Georgia

(b)(6)

In order to identify the HTTP headers, we need the packet capture to check if the requests' headers are the same on all these OPTIONS requests and unfortunately our pcap retention does not go that far.

In reference to office being the root cause of the traffic, I have noticed that the HTTP OPTIONS request does always precede an actual GET request to the same resource or to a resource in the same folder as the OPTIONS request and that the user Agent for the GET is either "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E; InfoPath.3; Tablet PC 2.0; IE8Mercury; ms-office) à (Office 2010)" OR "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 15)à (office 2013)". In order to confirm the hypothesis; I have pulled multiple proxy log samples (unrelated to SEN 2016-12-093) of traffic where User Agent string =" Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; Tablet PC 2.0; C15IE72011A; ms-office)" and sure enough there was an OPTIONS request made right before the GET. The other fact is that this UA is only seeing in ICE/CIS Network and based on my phone conversation with their SOC, they have stated that they do use tablet-PC and have office 2010.

We are still working on identifying what and how is the traffic generated with UA "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; Tablet PC 2.0; C15IE72011A; ms-office)" which would then explain the HTTP OPTIONS requests.



Obtained via FOIA by Judicial Watch, Inc.

Please let me know if you need more clarifications.

V/r,

(b)(6) (b)(6) GCIA, CNDA/CEH, CCNA Sec
Information Security Analyst
Critical Solutions Inc
Supporting the Enterprise Security Operations Center (ESOC)
Department of Homeland Security
MGMT/OCIO/CISO/SOC
DHS SOC COOP: (540) 542-(b)(6)

dhs_esoc_2_info

From: (b)(6) (b)(6) (CTR)
Sent: Tuesday, December 13, 2016 11:38 PM
To: (b)(6) (b)(6) (CTR) (b)(6) (b)(6) (b)(6) (b)(6)
Rohner, Boyden (b)(6) (b)(6) (b)(6) (b)(6)
(b)(6) (b)((b)(6)
Cc: (b)(6) (b)(6) (CTR) (b)(6) DHS ESOC Analysts
(b)(6)
Subject: RE: Update State of Georgia

Also, can we validate that each event involved opening a document on the Web site.
Thanks again -K

From: (b)(6) (b)(6) (CTR)
Sent: Tuesday, December 13, 2016 11:34:49 PM
To: (b)(6) (b)(6) Rohner, Boyden; (b)(6) (b)(6) (b)(6) (b)(

Obtained via FOIA by Judicial Watch, Inc.

Cc: (b)(6) (b)(6) (CTR); DHS ESOC Analysts
Subject: RE: Update State of Georgia

(b)(6)
One additional data point would help. Can we get what versions of MS Office were on the clients. I have been researching the OPTIONS command and having the Office version, especially in research on how the command is used.
Thanks (b)(6)

From: (b)(6) (b)(6
Sent: Tuesday, December 13, 2016 10:51:31 PM
To: Rohner, Boyden; (b)(6) (b)(6) (b)(6) (b)(
Cc: (b)(6) (b)(6) (CTR); DHS ESOC Analysts; (b)(6) (b)(6) (CTR)
Subject: Update State of Georgia

Good Evening Team,

From our most recent analysis, the new scanning events outlined in the GASOS letter appears to be additional "OPTIONS" request methods coming from the DHS IP space. We currently have splunk web logs showing these events from the Sep 12th event on. The events are as follows:

September 12, 2016 12:52:32 EDT (11:52 CDT)
Host **10.61.22.222** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.georgia.gov/ (Denied)

September 28, 2016 08:54:15 EDT (07:54 CDT)
Host **10.56.189.94** (ICE-CIS) attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://sos.ga.gov/index.php/licensing/plb/ (Denied)

October 3, 2016 11:41:32 EDT (10:41 CDT)
Host **10.101.194.178** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.state.ga.us/corporations/ (Denied)

October 6, 2016 11:14:16 EDT (10:14 CDT)
Host **10.32.82.42** (FEMA)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://verify.sos.ga.gov/verification/stylesheets/ (Observed)

November 7, 2016 13:15:43 EST (12:15 CST)
Host **10.56.189.65** (ICE-CIS)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://www.sos.georgia.gov/plb/cosmetology/ (Denied)

November 8, 2016 08:35:21 EST (07:35 CST)
Host **10.243.15.188** (FLETC)attempted **OPTIONS** via **Microsoft Office Protocol Discovery** to http://verify.sos.ga.gov/verification/stylesheets/ (Observed)

Unfortunately, our Splunk data does not go back as far as February and May. In addition our Einstein Data is not yielding any results (b)(6) is still working it). We have asked all the major components to

Obtained via FOIA by Judicial Watch, Inc.

check their logs for OPTIONS requests going to any GA websites on the remaining “Scan” dates in February and (b)(6) and the night shift will call all the SOCs to ensure they received the message).

Even if they do not yield any results, our other results fit a distinct and precise pattern of traffic. It would be very hard for them to repudiate the findings as anything other than non-malicious Microsoft OPTIONS requests. We will update and brief the Components again at 0900 tomorrow.

I will be following up with the Microsoft team shortly to try and expedite a response on their behalf.

Please feel free to add any additional findings or comments to this thread.

Respectfully,

(b)(6) (b)(6)

Sender:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Recipient:	(b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Boyden.rohner>"; (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DHS ESOC Analystsffd"
Sent Date:	2016/12/14 07:54:00
Delivered Date:	2016/12/14 07:54:01

Obtained via FOIA by Judicial Watch, Inc.

From:	Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
To:	(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Driggers, (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(M </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DUSCyberc93"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)"; "Lilly, Tamara </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Tamara.lilly>"; (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Gibson, (b)(6) M </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) L </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) Jeffery W </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Manfra, Jeanette </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Jeanette.manfra>"; (b)(6) (b)(6 </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Moran, (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Sutherland, Daniel </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) (b)(6 (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6)
CC:	(b)(6) (b)(6 </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Subject:	Update on Ga investigation
Date:	2016/12/14 17:27:01
Start Date:	2016/12/14 17:30:00
End Date:	2016/12/14 18:30:00
Priority:	Normal
Type:	Schedule.Meeting.Request
Location:	Teleconference: 866-903-0713 Pin: 2834417

Obtained via FOIA by Judicial Watch, Inc.

Attendees:	(b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6) (b)(6 Driggers, (b)(6) (b)(6) (b)(6 M; DUSCyber; (b)(Lilly, Tamara; (b)(6) (b)((b)(6) (b)(6) (b) (b)(6) (b)(6) L; (b)(6) (b)(6) Manfra, Jeanette; (b)(6) (b)(6) (b)(6) (b)((b)(6) (b)(6 (CTR); (b)(6) (b)(6) Sutherland, Daniel; (b)(6) (b)(6 DHS ESOC; (b)(6) (b)(6) (b)(6) (b)(6 (CTR); (b)(6)

Good afternoon,

The DHS ESOC will provide an update on the investigation into the Georgia Secretary of State's (GASOS) reports of DHS penetration attempts. Please distribute to others I may have missed.

Agenda:
-Investigation update (Boyden Rohner, Director Security Operations)
-Technical update (b)(6) (b)(6) ESOC Chief)
-Next steps
-Updates on inquiries from other States (Boyden Rohner)
-Questions

Sender:	Rohner, Boyden </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Recipient:	(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) "(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) "(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Driggers, Richard </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Richard.Driggers>"; (b)(6) (b)(6 M </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "/O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=DUSCyberc93"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) >"; "Lilly, Tamara </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Tamara.lilly>"; (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Gibson, (b)(6) M </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) L </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) Jeffery W </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP

Obtained via FOIA by Judicial Watch, Inc.

	(b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(</O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Moran, (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "Sutherland, Daniel </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) (b)(6) (b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6) (b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Sent Date:	2016/12/14 17:26:59
Delivered Date:	2016/12/14 17:27:01