



United States Department of State

Washington, D.C. 20520

October 24, 2016

Case No. F-2015-12809

Segment: IPS-0001

Mr. Michael Bekesha  
Judicial Watch  
425 Third St. SW. Suite 800  
Washington, DC 20024

Dear Mr. Bekesha:

I refer to our letter dated October 12, 2016 regarding the release of certain Department of State records under the Freedom of Information Act (the "FOIA"), 5 U.S.C. § 552.

The search of the materials provided to the Department by the FBI is completed. Our review of those records resulted in the identification of seven documents responsive to your request. After reviewing these documents, we previously released six documents and determined that one document required coordination with another agency. The interagency coordination has been completed, and we have determined that the document may be released with excisions.

An enclosure explains the FOIA exemptions and other grounds for withholding material. Where we have made excisions, the applicable FOIA exemptions are marked on the document. All non-exempt information that is reasonably segregable from the exempt material has been released. All released material is enclosed.

If you have any questions, your attorney may contact Trial Attorney, Jason Lee, U.S. Department of Justice, Civil Division, Federal Programs Branch, at (202) 514-3367 or [Jason.Lee3@usdoj.gov](mailto:Jason.Lee3@usdoj.gov). Please refer to the case number, shown above, and the civil action number, 15-cv-01441-JEB, in all communication about this case.

Sincerely,

A handwritten signature in black ink that reads "Eric F. Stein" followed by "for" in a smaller, less legible script.

Eric F. Stein, Acting Director  
Office of Information Programs and Services

Enclosures: As stated

## EXPLANATION OF GROUNDS FOR WITHHOLDING

### The Freedom of Information Act (FOIA) Exemptions (5 USC 552)

(b)(1) Withholding specifically authorized under an Executive Order in the interest of national defense or foreign policy, and properly classified.

#### Executive Order 12958, as amended, Classification Categories:

- 1.4(a) Military plans, systems or operations
- 1.4(b) Foreign government information
- 1.4(c) Intelligence activities, sources or methods, or cryptology
- 1.4(d) Foreign relations or foreign activities of the US including confidential sources
- 1.4(e) Scientific, technological or economic matters relating to national security, including defense against transnational terrorism
- 1.4(f) USG programs for safeguarding nuclear materials or facilities
- 1.4(g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to US national security, including defense against transnational terrorism
- 1.4(h) Information on weapons of mass destruction

(b)(2) Related solely to the internal personnel rules and practices of an agency.

(b)(3) Specifically exempted from disclosure by statute (other than section 552b of Title 5), e.g.:

- INA Immigration and Nationality Act, Title 8 USC Section 1202(f)
- CIA Central Intelligence Agency Act of 1949, Title 50 USC Section 403(g)
- ARMEX Arms Export Control Act, Title 22 USC 2778(e)
- EXPORT Export Administration Act of 1979, 50 App. USC 2411(c)(1)

(b)(4) Privileged/confidential trade secrets, commercial or financial information from a person.

(b)(5) Interagency or intra-agency communications forming part of the deliberative process, attorney client privilege, or attorney work product.

(b)(6) Release would constitute a clearly unwarranted invasion of personal privacy.

(b)(7) Information compiled for law enforcement purposes that would:

- (A) Interfere with enforcement proceedings.
- (B) Deprive a person of a fair trial.
- (C) Constitute an unwarranted invasion of personal privacy.
- (D) Disclose confidential sources.
- (E) Disclose investigation techniques.
- (F) Endanger life or physical safety of any individual.

NR Material not responsive to your FOIA request, excised in accordance with our agreement.

### Privacy Act Grounds for Withholding (5 USC 552a)

(d)(5) Information compiled in reasonable anticipation of a civil action proceeding.

(j)(1) CIA records.

(j)(2) Enforcement of criminal law, including efforts to prevent, control, or reduce crime or apprehend criminals, except records of arrest.

(k)(1) Classified pursuant to E.O. 12958 in the interest of national defense or foreign policy such as intelligence sources and methods.

(k)(2) Investigatory material compiled for law enforcement purposes.

(k)(3) Regarding protective services to the President of the US or other individual pursuant to Title 18, USC, Section 3056.

(k)(4) Required by statute to be maintained and used solely as statistical records.

(k)(5) Investigatory material compiled solely for the purpose of determining suitability eligibility or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his identity would be held in confidence.

(k)(6) Testing or exam material used to determine individual qualifications for appointment or promotion in Federal service, the release of which would compromise the testing or exam process.

(k)(7) Material used to determine potential for promotion in the armed services.

pp Information about another person or persons which does not constitute a record about the requester as defined in the access provision of the Privacy Act (section (d) (1)) and which may not be released except pursuant to a written request or with the prior written consent of the person or persons concerned (section (b)).

NR Material not responsive to your Privacy Act request.

**From:** [redacted]  
**Sent:** Tuesday, November 30, 2010 5:40 PM  
**To:** [redacted]  
**Subject:** Re: Fwd:

B7(C)

B7(C)

Copy, thanks for the update, Will d.

**REFERRED FOR CONSULTATION - USSS**

**From:** [redacted]  
**To:** Justin [redacted]  
**Cc:** [redacted]  
**Sent:** Tue Nov 30 17:36:40 2010  
**Subject:** Re: Fwd:

B7(C)

B6

B7(C)

Justin - FYI: I finally returned to house after much needed updates to software I'm using - It took awhile / Just logged into your account with success in case you see anything / about to retrieve data now...

Regards

[redacted]

B7(C)

**From:** Justin Cooper [redacted]  
**To:** [redacted]  
**Sent:** Tue Nov 30 12:28:41 2010  
**Subject:** Fwd:

B6

B7(C)

FYI

Begin forwarded message:

**From:** Bryan Pagliano [redacted]  
**Date:** November 30, 2010 12:22:55 AM EST  
**To:** Justin Cooper <[redacted]>  
**Subject:** Re:

B6

B6

Weird, looks like the attack came from 208.67.222.222 and started around 5pm.

It is a company called OpenDNS, they are a fairly reputable organization.

The traffic seems to have cleared up at about 11:50pm. I wonder if they figured out they had someone launching an attack from their servers.

This may also explain the DNS issue we had earlier. Might have been an injection attack launched from their servers prior to this denial of service attack. We use their servers to resolve external websites for both the sbs and the blackberry server so we'd be susceptible to such an attack. Would be a great launching point. There has been something up with DNS servers in the past few days. Comcast actually had theirs go down over the weekend for the whole east coast.

I looked into the logs for today at around 5:50pm for failed logon attempts was attempts from someone trying to use the huma username using firefox, coming from [redacted] which is a state department IP address. So likely that was huma making those attempts.

B7(E)

I have to hit the hay, but I can look into the failed logon attempts from the 27th tomorrow if it turns out that they were not doug.

Attached are some reports from symantec showing the denial of service attack that it detected. The pie chart shows the IP they came from and the graph shows when they occurred tonight. I checked opendns's web page and did not see an incident report, they might have one tomorrow... hopefully. If they start hitting us again, we can always block them with the firewall and use another DNS provider.

I have worked about 2 hours so far on this issue the past few days.

-Bryan

On Mon, Nov 29, 2010 at 11:03 PM, Bryan Pagliano [redacted] wrote:

B6

It would most likely be them logging in at [mail.clintonemail.com](mailto:mail.clintonemail.com) or [mail.presidentclinton.com](mailto:mail.presidentclinton.com)

On the web.

On Mon, Nov 29, 2010 at 10:51 PM, Justin Cooper [redacted] wrote:

B6

When u say log on.... To the server or their email?

----- Original Message -----

From: Bryan Pagliano [redacted]

B6

To: Justin Cooper

Sent: Mon Nov 29 22:48:31 2010

Subject: Re:

So to update you...

The failed logon attempts on the 27th were for username doug and dougband, the failed logon attempts on the 29th were for username huma. Would be useful to know if it was them who tried to log in.

Symantec logged a denial of service attack on the main server which could be a usual occurrence,, but I am looking into it. I can't tell yet if the pix (firewall) is picking this up too, I looking through the logs a bit more, but things are running slow, seems like the internet connection is getting clogged up.

It would be useful to know if the ISP is seeing any denial of service traffic from them across the internet wire if you are able to call them or call me with their info. [redacted]

B6

-Bryan

On Mon, Nov 29, 2010 at 5:36 PM, Justin Cooper [redacted] wrote:

B6

Begin forwarded message:

From: Bryan Pagliano [redacted]

Date: November 29, 2010 5:16:37 PM EST

To: Justin Cooper [redacted]

Subject: **\*\*Failed logon attempt\*\*** (Do Not reply)

There was a failed logon attempt logged on the server. To check who it was log onto the server and double click on the toolbox icon labeled Failed\_Logon\_Attempt. Then expand computer manager, then system tools, then event viewer, then windows logs, then click on security and look for an audit failure. Double click the audit failure and in the details it will list the account that failed to logon

Begin forwarded message:

From: Bryan Pagliano [redacted]

Date: November 29, 2010 5:16:36 PM EST

To: Justin Cooper [redacted]

Subject: **\*\*Failed logon attempt\*\*** (Do Not reply)

There was a failed logon attempt logged on the server. To check who it was log onto the server and double click on the toolbox icon labeled Failed\_Logon\_Attempt. Then expand computer manager, then system tools, then event viewer, then windows logs, then click on security and look for an audit failure. Double click the audit failure and in the details it will list the account that failed to logon

Begin forwarded message:

From: Bryan Pagliano [redacted]

Date: November 27, 2010 6:39:23 PM EST

To: Justin Cooper [redacted]

Subject: **\*\*Failed logon attempt\*\*** (Do Not reply)

There was a failed logon attempt logged on the server. To check who it was log onto the server and double click on the toolbox icon labeled Failed\_Logon\_Attempt. Then expand computer manager, then system tools, then event viewer, then windows logs, then click on security and look for an audit failure. Double click the audit failure and in the details it will list the account that failed to logon

Begin forwarded message:

From: Bryan Pagliano [redacted]

B6

Date: November 27, 2010 6:39:18 PM EST

To: Justin Cooper [redacted]

Subject: **\*\*Failed logon attempt\*\*** (Do Not reply)

There was a failed logon attempt logged on the server. To check who it was log onto the server and double click on the toolbox icon labeled Failed\_Logon\_Attempt. Then expand computer manager, then system tools, then event viewer, then windows logs, then click on security and look for an audit failure. Double click the audit failure and in the details it will list the account that failed to logon

Begin forwarded message:

From: Bryan Pagliano [redacted]

Date: November 27, 2010 6:38:51 PM EST

To: Justin Cooper [redacted]

Subject: **\*\*Failed logon attempt\*\*** (Do Not reply)

There was a failed logon attempt logged on the server. To check who it was log onto the server and double click on the toolbox icon labeled Failed\_Logon\_Attempt. Then expand computer manager, then system tools, then event viewer, then windows logs, then click on security and look for an audit failure. Double click the audit failure and in the details it will list the account that failed to logon

Begin forwarded message:

From: Bryan Pagliano [redacted]

Date: November 27, 2010 6:38:39 PM EST

To: Justin Cooper <[redacted]>

B6

Subject: **\*\*Failed logon attempt\*\*** (Do Not reply)

There was a failed logon attempt logged on the server. To check who it was log onto the server and double click on the toolbox icon labeled Failed\_Logon\_Attempt. Then expand computer manager, then system tools, then event viewer, then windows logs, then click on security and look for an audit failure. Double click the audit failure and in the details it will list the account that failed to logon

Begin forwarded message:

From: Bryan Pagliano <[redacted]>

Date: November 27, 2010 6:38:11 PM EST

To: Justin Cooper <[redacted]>

Subject: **\*\*Failed logon attempt\*\*** (Do Not reply)

There was a failed logon attempt logged on the server. To check who it was log onto the server and double click on the toolbox icon labeled Failed\_Logon\_Attempt. Then expand computer manager, then system tools, then event viewer, then windows logs, then click on security and look for an audit failure. Double click the audit failure and in the details it will list the account that failed to logon

Begin forwarded message:

From: Bryan Pagliano <[redacted]>

Date: November 27, 2010 9:53:50 AM EST

To: Justin Cooper <[redacted]>

Subject: **\*\*Failed logon attempt\*\*** (Do Not reply)

There was a failed logon attempt logged on the server. To check who it was log onto the server and double click on the toolbox icon labeled Failed\_Logon\_Attempt. Then expand computer manager, then system tools, then event viewer, then windows logs, then click on security and look for an audit failure. Double click the audit failure and in the details it will list the account that failed to logon

Begin forwarded message:

From: Bryan Pagliano [REDACTED]

B6

Date: November 27, 2010 9:53:41 AM EST

To: Justin Cooper [REDACTED]

Subject: **\*\*Failed logon attempt\*\*** (Do Not reply)

There was a failed logon attempt logged on the server. To check who it was log onto the server and double click on the toolbox icon labeled Failed\_Logon\_Attempt. Then expand computer manager, then system tools, then event viewer, then windows logs, then click on security and look for an audit failure. Double click the audit failure and in the details it will list the account that failed to logon