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:**

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