[redacted]

Department of Homeland Security (DHS)
DHS OneNet Security Operations Center (SOC)

Incident Report

Incident Number: 2012-09-039-External Auto-Forwarded Email

Incident Number: 2012-09-039-External Auto-Forwarded Email
Incident Type: Alteration/Compromise of Information
Component: CBP
City: **State:**
Status Description: CBP reports that one (1) CBP user had an auto-forwarding rule setup to have emails sent externally to a civilian's personal Gmail account. There is a possibility that sensitive information to include Personally Identifiable Information (PII) has been accidently sent out due to this rule. The incident was discovered when a civilian responded to a CBP user's email to a distribution list of other CBP/DHS users. The CBP user noticed the civilian's Gmail address and reported it to the FTO who then reported the incident to the CBP CSIRC. Upon investigation and confirmation from EaaS, one (1) CBP Border Patrol Agent who was on the email distribution list had an auto-forwarding rule setup within their Exchange account to a non-CBP/DHS user's personal Gmail account. The name of the Border Patrol Agent and the civilian are very similar, but it was determined that the Border Patrol Agent misconfigured the rule by using the civilian's personal Gmail address instead of his own. Technical remediation will include working with the EaaS team to implement a rule to disable the auto-forwarding rule and only allow it when requests are made to the Exchange team. The incident has been reported to the CBP Privacy Office and Joint Intake Center for action (assisting the user to have all government emails removed and confirmed).
Priority Level: 3
Criticality: Significant
Number of Systems Affected Level: 1
CIP Asset?: No
DHS Financial System?: No

Incident Log:

(b)(5),(b)(6),(b)(3):6 U.S.C. § 131(3) Protected Critical Infrastructures Information (PCII)

[redacted]

[redacted]

Department of Homeland Security (DHS)
DHS OneNet Security Operations Center (SOC)

Incident Report

Incident Number: 2012-10-013-Unauthorized access to Outlook

Incident Number: 2012-10-013-Unauthorized access to Outlook
Incident Type: Alteration/Compromise of Information
Component: Master
City: **State:**
Status Description: CBP reports that during the EAAS migration several CBP users have been given access to sensitive files for which the users did not have access prior. These files contain information from Internal Affairs, Personnel folders, FEMA, White House meetings, Diplomatic Meetings, and emails from upper management. Remediation action required includes the locking down of access to these files.
Priority Level: 3
Criticality: Significant
Number of Systems Affected Level: 1
CIP Asset?: No
DHS Financial System?: No

Incident Log:

(b)(5),(b)(6),(b)(3):6 U.S.C. § 131(3) Protected Critical Infrastructures Information (PCII)

[redacted]

[redacted]

Department of Homeland Security (DHS)
DHS OneNet Security Operations Center (SOC)

Incident Report

Incident Number: 2012-10-036-External Auto-Forwarded Emails

Incident Number: 2012-10-036-External Auto-Forwarded Emails
Incident Type: Misuse
Component: Master
City: **State:**
Status Description: DHS SOC reports that a total of 771 rules are configured in Exchange to auto-forward emails external to DHS. DHS SOC requested and received a list of 771 automated email forwarding rules created by DHS Email as a Service (EaaS) users. Auto-forwarding or redirecting of DHS email to address outside of the .gov or .mil domain is prohibited and shall not be used per DHS 4300A policy, section 5.4.6.i and poses a high risk of accidental disclosure of PII, SBU, FOUO, LES, or classified data. The incident has been reported to the Joint Intake Center (JIC). Affected Components (CBP, FEMA, DHS HQ, and DC2) are asked to identify and remediate the rules.
Priority Level: 3
Criticality: Significant
Number of Systems Affected Level: 771
CIP Asset?: No
DHS Financial System?: No

Incident Log:

(b)(5),(b)(6),(b)(3):6 U.S.C. § 131(3) Protected Critical Infrastructures Information (PCII)

[redacted]

[redacted]

Department of Homeland Security (DHS)
DHS OneNet Security Operations Center (SOC)

Incident Report

Incident Number: 2013-07-168-OutlookPublicFolders

Incident Number: 2013-07-168-OutlookPublicFolders
Incident Type: Alteration/Compromise of Information
Component: Master
City: **State:**
Status Description: DHS SOC was made aware of PII and SBU information that are readily available on some of the public folders on Outlook exchange servers. A local FTO contacted DHS SOC to report that he/she has discovered that he/she has full access to documents/emails containing PII information and other potentially sensitive but unclassified information located on various public folders on Oulook Exchange servers. Cursory investigation of the folders shows that the information available includes Names, DOB, A-number, TECS record ID, TECS status, internal procedure memos, etc. Investigation is ongoing to determine the full scope of the incident.
Priority Level: 3
Criticality: Minor
Number of Systems Affected Level: 1
CIP Asset?: No
DHS Financial System?: No

Incident Log:

(b)(5),(b)(6),(b)(3):6 U.S.C. § 131(3) Protected Critical Infrastructures Information (PCII)

[redacted]

[redacted]

Department of Homeland Security (DHS)
DHS OneNet Security Operations Center (SOC)

Incident Report

Incident Number: 2013-10-160-Alteration/Compromise of Information

Incident Number: 2013-10-160-Alteration/Compromise of Information
Incident Type: Alteration/Compromise of Information
Component: DC1
City: (b)(6)
Status Description: DC1 reports that one (1) ISSO noticed the WPaaS Engineers are still using the same username and password that was exposed on the Change Request 8852 documentation. The Change Request 8852 had exposed the SNMP community strings commands username and passwords. The first occurrence for this security event is documented on SEN #2013-07-117 and the SEN was closed on 07/17/2013. Investigation ongoing...

Priority Level: 3
Criticality: Minor
Number of Systems Affected Level: 1
CIP Asset?: No
DHS Financial System?: No

Incident Log:

(b)(5),(b)(6),(b)(3):6 U.S.C. § 131(3) Protected Critical Infrastructures Information (PCII)

[redacted]

[redacted]

Department of Homeland Security (DHS)
DHS OneNet Security Operations Center (SOC)

Incident Report

Incident Number: 2014-06-030-CGPC-EPM-2

Incident Number: 2014-06-030-CGPC-EPM-2
Incident Type: Alteration/Compromise of Information
Component: USCG
City: ARLINGTON **State:** VA
Status Description: USCG reports that one (1) PDF document containing the Personal Identifiable Information of one thousands (1000) individuals was published on the USCG public facing Internet website. Investigation confirmed that the PII included the names of personnel, their duty station location as well as their duty and medical hold status. Remediation efforts taken included removing the PDF document off of the USCG WWW Internet Staging and Production Servers and submitting a formal request to have the cached version of the PDF document removed from [redacted] USCG privacy office was be engaged for further guidance.
(b)(3):6 U.S.C. § 131(3) Protected Critica
Priority Level: 3
Criticality: Significant
Number of Systems Affected Level: 2
CIP Asset?: No
DHS Financial System?: No

Incident Log:

(b)(5),(b)(6),(b)(3):6 U.S.C. § 131(3) Protected Critical Infrastructures Information (PCII)

[redacted]