MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Records/Information - Obtained
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
February 1, 2021	February 2, 2021	875 15th Street, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
Government Security Operations Center, soc@gsoc.treas.gov		(b) (6), (b) (7)(C), Senior Special Agent

On February 1, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) received a list of email accounts which were bound to other accounts via the FolderBind method. The list was provided by Treasury's Government Security Operations Center (GSOC).

The FolderBind operation allows one user access to another's mailbox. In the data provided by GSOC, the FolderBind operation indicated account name (b) (6), (b) (7)(C) had access to about 319 other Treasury email accounts (Attachment 1). (b) (6), (b) (7)(C) account had "FullAccess" permissions. This indicates the (b) (6), (b) (7)(C) account could read, write, edit, and delete information in the other users' mailboxes.

Attachments:
1. (b) (6), (b) (MailboxPerms.csv

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

User		AccessRights	Identity
(b)(6)	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	Arcadi, Tony
	@treasury.gov	FullAccess	Haarsager, Mathew
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	Turner, Kay
	@treasury.gov	FullAccess	(b)(6)

(b)(6)	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	Lee, Albert
	@treasury.gov	FullAccess	Orlando, Jason
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	

(b)(6)	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	Sturm Jr, Rex (Logan)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	Postmaster1
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	

(b)(6)	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	McDonald, Larry
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	Moravec, Charles
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	

(b)(6)	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	Kaplan, Michael
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	

(b)(6)	@treasury.gov	FullAccess	GSOCTesting
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	Mohlenkamp, Matthew
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	

(b)(6)	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	

(b)(6)	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	OIA_IRMO
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	

(b)(6)	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(Contractor)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(Contractor)
	@treasury.gov	FullAccess	Baukol, Andrew
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	

(b)(6)	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	

(b)(6)	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	McCauley, Brian
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	Totten, Nicolaos
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	Zuckerman, Amy
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)

(b)(6)	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	

(b)(6)	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	Yang, Sharon
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	Moghtader, Lailee
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)

(b)(6)	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	(b)(6) Contractor)
	@treasury.gov	FullAccess	(Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	Reissaus, Brian
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6) (Contractor)
	@treasury.gov	FullAccess	(b)(6)
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	
	@treasury.gov	FullAccess	(b)(6) (Contractor)

(b)(6)	@treasury.gov	FullAccess	(b)(6)	(Contractor)
	@treasury.gov	FullAccess		
	@treasury.gov	FullAccess	(b)(6)	
	@treasury.gov	FullAccess		
	@treasury.gov	FullAccess		
	@treasury.gov	FullAccess		
	@treasury.gov	FullAccess		
	@treasury.gov	FullAccess		
	@treasury.gov	FullAccess		
	@treasury.gov	FullAccess		
	@treasury.gov	FullAccess		
	@treasury.gov	FullAccess		

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Records/Information - Obtained
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
February 10, 2021	February 12, 2021	875 15th Street, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) [redacted]		(b) (6), (b) (7)(C), Senior Special Agent (b) (6), (b) (7)(C), Senior Special Agent

On February 10, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) received a spreadsheet containing a list of about 300 email accounts which were previously identified as accessible via FolderBind permissions. The compromised account (b) (6), (b) (7)(C) [redacted] was granted FolderBind access to each of the aforementioned email accounts (Attachment 1).

The spreadsheet includes a breakdown of impacted accounts, by office. About 56% of the affected account holders were assigned to Information Systems and HR Connect. The Office of International Affairs accounted for 37% of the vulnerable accounts and Terrorism and Financial Intelligence, 3%.

Attachments:
1. UPDATED OCI_Microsoft FolderBinds 8 Feb 2021_Secured.xlsx

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

Office Name	Number of Impacted Accounts	Percent of Total Impacted Accounts
Chief Information Officer (CIO)	178	56%
Information Systems	115	36%
HR Connect Program Office (HRCPO)	63	20%
International Affairs (IA)	117	37%
International Finance	53	17%
International Markets and Development	49	16%
Office of the Under Secretary of IA	15	5%
Terrorism and Financial Intelligence (TFI)	10	3%
Office of Foreign Asset Control (OFAC)	8	<3%
Office of Intelligence and Analysis (OIA)	2	1%
Management	3	1%
Treasury Operations	2	1%
Office of the Assistant Secretary for Management	1	<1%
N/A	8	3%
Total	**316**	**100%**

Name	Position	Sub-Office	Office
(b)(6)	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Contractor	HR Connect Program Office (HRCPO)	CIO
	Customer Service Analyst	HR Connect Program Office (HRCPO)	CIO
	Customer Service Analyst	HR Connect Program Office (HRCPO)	CIO
	Customer Support Analyst	HR Connect Program Office (HRCPO)	CIO
	Data Management Analyst	HR Connect Program Office (HRCPO)	CIO
	Detailee	HR Connect Program Office (HRCPO)	CIO
	Director, Business Operations	HR Connect Program Office (HRCPO)	CIO
	Director, EBS Service Portfolio Management	HR Connect Program Office (HRCPO)	CIO
	Director, Enterprise Content & Case Management (ECM)	HR Connect Program Office (HRCPO)	CIO
	EBS Enterprise Application Cybersecurity ISSM	HR Connect Program Office (HRCPO)	CIO
	Functional Analyst	HR Connect Program Office (HRCPO)	CIO
	Functional Analyst	HR Connect Program Office (HRCPO)	CIO
	HR IT Project Manager	HR Connect Program Office (HRCPO)	CIO
	HR IT Project Manager	HR Connect Program Office (HRCPO)	CIO
	Information Systems Security Manager	HR Connect Program Office (HRCPO)	CIO
	IT Quality Assurance Project Manager	HR Connect Program Office (HRCPO)	CIO
	IT Specialist	HR Connect Program Office (HRCPO)	CIO
	IT Specialist	HR Connect Program Office (HRCPO)	CIO

(b)(6)	IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Applications Software	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Applications Software	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Applications Software	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Applications Software	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Customer Support	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Data Management	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Network	HR Connect Program Office (HRCPO)	CIO
	IT Specialist, Web Developer	HR Connect Program Office (HRCPO)	CIO
	Payroll Product Manager	HR Connect Program Office (HRCPO)	CIO
	Program Analyst, CareerConnector	HR Connect Program Office (HRCPO)	CIO
	Program Manager	HR Connect Program Office (HRCPO)	CIO
	Project Manager	HR Connect Program Office (HRCPO)	CIO
	Project Manager	HR Connect Program Office (HRCPO)	CIO
	Project Resource Analyst	HR Connect Program Office (HRCPO)	CIO
	Project Resource Analyst	HR Connect Program Office (HRCPO)	CIO
(b)(6)	Senior Advisor	HR Connect Program Office (HRCPO)	CIO
	Senior Program Manager, Technology Applications Services	HR Connect Program Office (HRCPO)	CIO
	Senior Technical Advisor, CTO	HR Connect Program Office (HRCPO)	CIO
	Supervisory HR Specialist	HR Connect Program Office (HRCPO)	CIO
	Supervisory IT Project Manager	HR Connect Program Office (HRCPO)	CIO
	Supervisory IT Specialist, Information Security	HR Connect Program Office (HRCPO)	CIO
	Supervisory Project Manager	HR Connect Program Office (HRCPO)	CIO
	TLMS Platform Manager	HR Connect Program Office (HRCPO)	CIO
Tony Arcadi	ACIO Enterprise Infrastructure Operations Services	Information Systems	CIO
Nick Totten	ACIO for Enterprise Application Services	Information Systems	CIO
	Associate Director, Enterprise Networks	Information Systems	CIO
	Business Operations Manager	Information Systems	CIO
	Computer Support Tech	Information Systems	CIO
(b)(6)	Contractor	Information Systems	CIO
	Contractor	Information Systems	CIO
	Contractor	Information Systems	CIO
	Contractor	Information Systems	CIO

(b)(6)	Contractor	Information Systems	CIO
	Contractor	Information Systems	CIO
	Contractor	Information Systems	CIO

(b)(6)	Contractor	Information Systems	CIO
	Contractor	Information Systems	CIO
	Contractor	Information Systems	CIO
	Contractor	Information Systems	CIO
	Customer Support	Information Systems	CIO
	Customer Support Analyst	Information Systems	CIO
	Customer Support Analyst	Information Systems	CIO
	Data Center Operation Manager	Information Systems	CIO
	Director of Enterprise Engineering	Information Systems	CIO
	Director of Financial Systems Technology	Information Systems	CIO
	Director, Technology Discovery and Integration	Information Systems	CIO
	Enterprise Architect	Information Systems	CIO
	Enterprise Architect	Information Systems	CIO
	Financial Analyst	Information Systems	CIO
	Financial Manager	Information Systems	CIO
	GSOC	Information Systems	CIO
	GSOC	Information Systems	CIO
	GSOC	Information Systems	CIO
	GSOC	Information Systems	CIO
	HSPD-12 Project Management	Information Systems	CIO
	Information Technology Specialist	Information Systems	CIO
	IT Specialist	Information Systems	CIO
	IT Specialist	Information Systems	CIO
	IT Specialist	Information Systems	CIO
	IT Specialist	Information Systems	CIO
	IT Specialist	Information Systems	CIO
	IT Specialist	Information Systems	CIO
	IT Specialist	Information Systems	CIO
	IT Specialist, ICAM	Information Systems	CIO
	IT Specialist, Information Security	Information Systems	CIO
	IT Specialist, Information Security	Information Systems	CIO
	IT Specialist, Information Security	Information Systems	CIO
	IT Specialist, Information Security	Information Systems	CIO
	IT Specialist, Information Security	Information Systems	CIO
	IT Specialist, Information Security	Information Systems	CIO
	IT Specialist, Information Security	Information Systems	CIO
	IT Specialist, Information Security	Information Systems	CIO
	IT Specialist, Information Security	Information Systems	CIO
	IT Specialist, Information Security	Information Systems	CIO
	IT Specialist, Information Security	Information Systems	CIO

(b)(6)	IT Specialist, Information Security	Information Systems	CIO
	IT Specialist, Network Services	Information Systems	CIO
	IT Specialist, Network Services	Information Systems	CIO
	IT Specialist, Network Services	Information Systems	CIO
	IT Specialist, Operating Systems	Information Systems	CIO
	IT Specialist, System Administrator	Information Systems	CIO
	IT Specialist, System Administrator	Information Systems	CIO
	IT Specialist, System Administrator	Information Systems	CIO
	IT Specialist, Systems Aministrator	Information Systems	CIO
	Management Analyst	Information Systems	CIO
	Management and Program Analyst	Information Systems	CIO
	Management and Program Analyst	Information Systems	CIO
	Management and Program Analyst	Information Systems	CIO
	Management and Program Analyst	Information Systems	CIO
	PKI Policy Management Authority	Information Systems	CIO
	Program Analyst	Information Systems	CIO
	Service Desk Manager	Information Systems	CIO
	Supervisory IT Specialist, Customer Specialist	Information Systems	CIO
	Supervisory IT Specialist, Customer Specialist	Information Systems	CIO
	Supervisory IT Specialist, Customer Specialist	Information Systems	CIO
	Supervisory IT Specialist, Information Security	Information Systems	CIO
	Supervisory IT Specialist, Information Security	Information Systems	CIO
	Supervisory IT Specialist, Information Security	Information Systems	CIO
	System Administrator	Information Systems	CIO
	System Administrator	Information Systems	CIO
	TEICAM Program Director	Information Systems	CIO

Name	Position	Portfolio	Sub-Office	Office
(b)(6)	Deputy Director, Africa	Africa	International Finance	IA
	International Economist	Africa	International Finance	IA
	International Economist	Africa	International Finance	IA
	Office Director, African Nations	Africa	International Markets and Development	IA
	Senior International Health Economist	Africa	Office of the Under Secretary of IA	IA
	Associate Director, Budget	Budget	International Markets and Development	IA
Brian Reissaus	Director, Investment Security Office and Acting A/S CFIUS	CFIUS	International Markets and Development	IA
	Deputy Director, Office of Investment Security	CFIUS	International Markets and Development	IA
(b)(6)	Policy Advisor	CFIUS	International Markets and Development	IA
	Policy Advisor	CFIUS	International Markets and Development	IA
	Policy Advisor	CFIUS	International Markets and Development	IA
	Senior Case Officer	CFIUS	International Markets and Development	IA
	Supervisory International Economist, Deputy Office Director	CFIUS	International Markets and Development	IA
Brian McCauley	Supervisory International Economist, Deputy Office Director	CFIUS	International Markets and Development	IA
	Administrative Support Specialist	Development	International Markets and Development	IA
(b)(6)	Deputy Director, Development	Development	International Markets and Development	IA
	Director, Office of Development Results and Accountability	Development	International Markets and Development	IA
	International Economist	Development	International Markets and Development	IA
	Policy Advisor	Development	International Markets and Development	IA
	Policy Advisor	Development	International Markets and Development	IA
Mathew Haarsager	DAS, International Development Finance and Policy	Development	International Markets and Development	IA
	Director	East Asia	International Finance	IA
(b)(6)	International Economist	East Asia	International Finance	IA
	International Economist	East Asia	International Finance	IA
	Supervisory International Economist, Deputy Office Director	East Asia	International Finance	IA
	Supervisory International Economist, Deputy Office Director	East Asia	International Finance	IA
	Supervisory International Economist, Deputy Office Director	East Asia	International Finance	IA
	Treasury Attache	East Asia	International Finance	IA
(b)(6)	Supervisory International Economist, Deputy Office Director	East Asia	International Finance	IA
	Treasury Attache	East Asia	International Finance	IA
	Supervisory International Economist, Deputy Office Director	East Asia	International Markets and Development	IA
	Associate Director, Enforcement	Enforcement	International Markets and Development	IA
	Deputy Office Director	Financial Markets	International Finance	IA
(b)(6)	International Banking and Securities Markets	Financial Markets	International Finance	IA
	Supervisory International Economist, Deputy Office Director	Financial Markets	International Finance	IA
	Supervisory International Economist, Deputy Office Director	Financial Markets	International Finance	IA
	International Economist	Financial Markets	International Markets and Development	IA
Sharon Yang	DAS, Financial Markets	Financial Markets	Office of the Under Secretary of IA	IA
	Director, Office of Global Economics & Debt	Global Economics and Debt	International Finance	IA
(b)(6)	International Economist	Global Economics and Debt	International Finance	IA
	International Economist	Global Economics and Debt	International Finance	IA
(b)(6)	Supervisory International Economist, Deputy Office Director	Global Economics and Debt	International Finance	IA
	International Economist	Global Economics and Debt	International Markets and Development	IA
(b)(6)	Supervisory International Economist, Deputy Office Director	Global Economics and Debt	Office of the Under Secretary of IA	IA
	Associate Director, Government Debt	Government Debt	International Markets and Development	IA
Andy Baukol	PDAS and Acting Deputy Secretary, International Monetary Policy	International Monetary Policy	International Finance	IA
	Director, Office of International Monetary Policy	International Monetary Policy	International Finance	IA
(b)(6)	International Economist	International Monetary Policy	International Finance	IA
	International Economist	International Monetary Policy	International Markets and Development	IA
	International Economist	International Monetary Policy	International Markets and Development	IA
(b)(6)	Senior Advisor to the Under Secretary for IA	International Monetary Policy	Office of the Under Secretary of IA	IA
Albert Lee	Director, Markets Room	Market Room	International Finance	IA
	International Economist	Market Room	International Finance	IA
(b)(6)	Supervisory International Economist, Deputy Office Director	Market Room	International Finance	IA
	Deputy Director, Market Room	Market Room	Office of the Under Secretary of IA	IA
(b)(6)	Supervisory International Economist, Deputy Office Director	MDB	International Finance	IA
	Supervisory International Economist, Deputy Office Director	MDB	International Finance	IA
(b)(6)	International Economist	MDB	International Markets and Development	IA
	Deputy Director, Middle East and North Africa	Middle East & North Africa (MENA)	International Finance	IA

(b)(6)	Director, International Economics	Middle East & North Africa (MENA)	International Finance	IA
	Senior Advisor	Middle East & North Africa (MENA)	International Finance	IA
	Supervisory International Economist	Middle East & North Africa (MENA)	International Finance	IA
Eric Meyer	DAS, Africa and Middle East	Middle East & North Africa (MENA)	Office of the Under Secretary of IA	IA
Charles Moravec	Supervisory International Economist, Office of the Director	Mulilateral Development Bank	International Markets and Development	IA
	Deputy Office Director, Negotiations	Negotiations	International Markets and Development	IA
(b)(6)	International Economist	South East Asia	International Finance	IA
	International Economist	South East Asia	International Finance	IA
	International Economist	South East Asia	International Finance	IA
	Senior Policy Adviser to the Conselor to the Secretary	South East Asia	International Finance	IA
	Supervisory International Economist, Deputy Office Director	South East Asia	International Finance	IA
Matthew Mohlenkamp	Supervisory International Economist, Office Director of IA	South East Asia	International Finance	IA
Larry McDonald	DAS, Technical Assistance Policy	Technical Assistance	International Markets and Development	IA
Jason Orlando	Director, Technical Assistance	Technical Assistance	International Markets and Development	IA
	Director, Office of Trade and Investment Policy	Trade Policy	International Markets and Development	IA
(b)(6)	International Economist	Trade Policy	International Markets and Development	IA
	International Economist	Trade Policy	International Markets and Development	IA
	International Economist	Trade Policy	International Markets and Development	IA
	Supervisory International Economist, Deputy Office Director	Trade Policy	International Markets and Development	IA
Lailee Moghtader	DAS, Trade Policy	Trade Policy	Office of the Under Secretary of IA	IA
(b)(6)	International Economist	Trade Policy	Office of the Under Secretary of IA	IA
Michael Kaplan	DAS, Western Hemisphere & South Asia	Western Hemisphere	International Finance	IA
	International Economist	Western Hemisphere	International Finance	IA
	International Economist	Western Hemisphere	International Finance	IA
	Supervisory International Economist, Deputy Office Director	Western Hemisphere	International Finance	IA
(b)(6)	Supervisory International Economist, Deputy Office Director	Western Hemisphere	International Finance	IA
	Supervisory International Economist, Deputy Office Director	Western Hemisphere	International Finance	IA
	Administrative Support Specialist		International Finance	IA
	Administrative Support Specialist		International Finance	IA
	Administrative Support Specialist		International Finance	IA
(b)(6)	Administrative Support Specialist		International Finance	IA
	Administrative Support Specialist		International Finance	IA
	Administrative Support Specialist		International Finance	IA
	International Economist		International Finance	IA
	International Economist		International Finance	IA
	International Economist		International Finance	IA
	International Economist		International Finance	IA
	International Economist		International Finance	IA
	International Economist		International Finance	IA
	Supervisory International Economist, Deputy Office Director		International Finance	IA
	Accountant		International Markets and Development	IA
	Accountant		International Markets and Development	IA
	Contractor		International Markets and Development	IA
	Contractor		International Markets and Development	IA
	Financial Manager		International Markets and Development	IA
(b)(6)	International Economist		International Markets and Development	IA
	International Economist		International Markets and Development	IA
	International Economist		International Markets and Development	IA
	International Economist		International Markets and Development	IA
	International Economist		International Markets and Development	IA
	Investment Manager		International Markets and Development	IA
	Post Conflict Coordinator		International Markets and Development	IA
	Program Analysis Officer		International Markets and Development	IA
(b)(6)	Senior Case Officer		International Markets and Development	IA
	Travel Specialist		International Markets and Development	IA
	Deputy Office Director		Office of the Under Secretary of IA	IA
	Deputy Senior Director, Business & Program/Administrative Operations		Office of the Under Secretary of IA	IA
	Director, Business Opertions		Office of the Under Secretary of IA	IA
	Disclosure Coordinator and Information Analyst		Office of the Under Secretary of IA	IA
	Management and Program Analyst		Office of the Under Secretary of IA	IA

(b)(6)	Program Specialist, Special Events	Office of the Under Secretary of IA	IA
	Senior Administrative Office	Office of the Under Secretary of IA	IA

Name	Position	Sub-Office	Office
(b) (6), (b) (7)(C)		Office of Foreign Assets Control (OFAC)	TFI
		Office of Foreign Assets Control (OFAC)	TFI
		Office of Foreign Assets Control (OFAC)	TFI
		Office of Foreign Assets Control (OFAC)	TFI
		Office of Foreign Assets Control (OFAC)	TFI
		Office of Foreign Assets Control (OFAC)	TFI
		Office of Foreign Assets Control (OFAC)	TFI
		Office of Foreign Assets Control (OFAC)	TFI
		Office of Intelligence and Analysis (OIA)	TFI
		Office of Intelligence and Analysis (OIA)	TFI

Name	Position	Sub-Office	Office
(b)(6)	Digital Services Expert	Office of the Assistant Secretary for Management	Management
	Printing Services Specialist	Treasury Operations	Management
	Supervisory Printing Services Specialist	Treasury Operations	Management

Name	Email Address	Phone	Position	Sub-Office	Office	Focus
(b)(6)	(b)(6)@treasury.gov	(b)(6)	Enforcement Officer	Office of Foreign Assets Control (OFAC)	TFI	
	(b)(6)@treasury.gov		Enforcement Officer	Office of Foreign Assets Control (OFAC)	TFI	
	(b)(6)@treasury.gov		Enforcement Officer	Office of Foreign Assets Control (OFAC)	TFI	
	(b)(6)@treasury.gov		Management and Program Analyst	Office of Foreign Assets Control (OFAC)	TFI	
	(b)(6)@treasury.gov		Records and Information Management Specialist	Office of Foreign Assets Control (OFAC)	TFI	
	(b)(6)@treasury.gov		Records and Information Management Specialist	Office of Foreign Assets Control (OFAC)	TFI	
	(b)(6)@treasury.gov		Sanctions Licensing Officer	Office of Foreign Assets Control (OFAC)	TFI	
	(b)(6)@treasury.gov		Senior Advisor	Office of Foreign Assets Control (OFAC)	TFI	
OIA IRMO	IRMO_Communications@treasury.gov		Insider Risk Management Office (IRMO)	Office of Intelligence and Analysis (OIA)	TFI	
(b)(6)	(b)(6)@treasury.gov		Intelligence Analyst	Office of Intelligence and Analysis (OIA)	TFI	
	(b)(6)@treasury.gov	N/A	N/A	N/A	N/A	
	(b)(6)@treasury.gov	N/A	N/A	N/A	N/A	
	(b)(6)@treasury.gov	N/A	N/A	N/A	N/A	
	(b)(6)@treasury.gov	N/A	N/A	N/A	N/A	
	(b)(6)@treasury.gov	N/A	N/A	N/A	N/A	
	(b)(6)@treasury.gov	N/A	N/A	N/A	N/A	
	(b)(6)@treasury.gov	N/A	N/A	N/A	N/A	
(b)(6)	(b)(6)@treasury.gov	N/A	N/A	N/A	N/A	
(b)(6)	(b)(6)@treasury.gov	(b)(6)	Digital Services Expert	Office of the Assistant Secretary for Management	Management	
	(b)(6)@treasury.gov		Printing Services Specialist	Treasury Operations	Management	
	(b)(6)@treasury.gov		Supervisory Printing Services Specialist	Treasury Operations	Management	
	(b)(6)@treasury.gov		Administrative Support Specialist	International Finance	IA	
(b)(6)	(b)(6)@treasury.gov		Administrative Support Specialist	International Finance	IA	
	(b)(6)@treasury.gov		Administrative Support Specialist	International Finance	IA	
	(b)(6)@treasury.gov		Administrative Support Specialist	International Finance	IA	
Michael Kaplan	Michael.Kaplan@treasury.gov		DAS, Western Hemisphere & South Asia	International Finance	IA	
(b)(6)	(b)(6)@treasury.gov		Deputy Director, Africa	International Finance	IA	
	(b)(6)@treasury.gov		Deputy Director, Middle East and North Africa	International Finance	IA	
	(b)(6)@treasury.gov		Deputy Office Director	International Finance	IA	
	(b)(6)@treasury.gov		Director	International Finance	IA	
	(b)(6)@treasury.gov		Director, International Economics	International Finance	IA	
Albert Lee	Albert.Lee@treasury.gov		Director, Markets Room	International Finance	IA	
(b)(6)	(b)(6)@treasury.gov		Director, Office of Global Economics & Debt	International Finance	IA	
	(b)(6)@treasury.gov		Director, Office of International Monetary Policy	International Finance	IA	
	(b)(6)@treasury.gov		International Banking and Securities Markets	International Finance	IA	
	(b)(6)@treasury.gov		International Economist

(b)(6)	(b)(6)@treasury.gov	(b)(6)	International Economist	International Markets and Development	IA
	(b)(6)@treasury.gov		International Economist	International Markets and Development	IA
	(b)(6)@treasury.gov		International Economist	International Markets and Development	IA
	(b)(6)@treasury.gov		International Economist	International Markets and Development	IA
	(b)(6)@treasury.gov		Senior Case Officer	International Markets and Development	IA
Sharon Yang	Sharon.Yang@treasury.gov		DAS	Office of the Under Secretary of IA	IA
Eric Meyer	Eric.Meyer@treasury.gov		DAS, Africa and Middle East	Office of the Under Secretary of IA	IA
Lailee Moghtader	Lailee.Moghtader@treasury.gov		DAS, Trade Policy	Office of the Under Secretary of IA	IA
(b)(6)	(b)(6)@treasury.gov		Deputy Director	Office of the Under Secretary of IA	IA
	(b)(6)@treasury.gov		Deputy Office Director	Office of the Under Secretary of IA	IA
	(b)(6)@treasury.gov		Director, Business Opertions	Office of the Under Secretary of IA	IA
	(b)(6)@treasury.gov		Disclosure Coordinator and Information Analyst	Office of the Under Secretary of IA	IA
	(b)(6)@treasury.gov		International Economist	Office of the Under Secretary of IA	IA
	(b)(6)@treasury.gov		Management and Program Analyst	Office of the Under Secretary of IA	IA
	(b)(6)@treasury.gov		Senior Administrative Office	Office of the Under Secretary of IA	IA
(b)(6)	(b)(6)@treasury.gov		Senior Advisor to the Under Secretary for IA	Office of the Under Secretary of IA	IA
	(b)(6)@treasury.gov		Senior International Health Economist	Office of the Under Secretary of IA	IA
	(b)(6)@treasury.gov		Supervisory International Economist, Deputy Office Director	Office of the Under Secretary of IA	IA
	(b)(6)@treasury.gov		Deputy Senior Director, Business & Program/Administrative Operations	Office of the Under Secretary of IA	IA
	(b)(6)@treasury.gov		Program Specialist, Special Events	Office of the Under Secretary of IA	IA
	(b)(6)@treasury.gov		Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov	(b)(6)	Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov	N/A	Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov	(b)(6)	Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov	N/A	Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov	N/A	Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Contractor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Customer Service Analyst	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Customer Service Analyst	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Customer Support Analyst	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Data Management Analyst	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov	(b)(6)	Detailee	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Director, Business Operations	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Director, EBS Service Portfolio Management	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Director, Enterprise Content & Case Management (ECM)	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		EBS Enterprise Application Cybersecurity ISSM	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Functional Analyst	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Functional Analyst	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		HR IT Project Manager	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		HR IT Project Manager	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Information Systems Security Manager	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Quality Assurance Project Manager	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov	(b)(6)	IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Applications	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Applications Software	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Applications Software	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Applications Software	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Applications Software	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Customer Support	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Data Management	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		IT Specialist, Network	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov	(b)(6)	IT Specialist, Web Developer	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Payroll Product Manager	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Program Analyst, CareerConnector	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Program Manager	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Project Manager	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Project Manager	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Project Resource Analyst	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Project Resource Analyst	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Senior Advisor	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Senior Program Manager, Technology Applications Services	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Senior Technical Advisor, CTO	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Supervisory HR Specialist	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Supervisory IT Project Manager	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Supervisory IT Specialist, Information Security	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		Supervisory Project Manager	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov		TLMS Platform Manager	HR Connect Program Office (HRCPO)	CIO
	(b)(6)@treasury.gov	N/A		HR Connect Program Office (HRCPO)	CIO
Tony Arcadi	Tony.Arcadi@treasury.gov		ACIO Enterprise Infrastructure Operations Services	Information Systems	CIO
Nick Totten	Nick.Totten@treasury.gov		ACIO for Enterprise Application Services	Information Systems	CIO
	(b)(6)@treasury.gov	(b)(6)	Associate Director, Enterprise Networks	Information Systems	CIO
	(b)(6)@treasury.gov		Business Operations Manager	Information Systems	CIO
	(b)(6)@treasury.gov		Computer Support Tech	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	(b)(6)	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	(b)(6)	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	(b)(6)	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	(b)(6)	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	(b)(6)	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	(b)(6)	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov	(b)(6)	Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO
	(b)(6)@treasury.gov		Contractor	Information Systems	CIO

(b)(6)@treasury.gov	(b)(6)	Contractor	Information Systems	CIO
(b)(6)@treasury.gov		Contractor	Information Systems	CIO
(b)(6)@treasury.gov	(b)(6)	Contractor	Information Systems	CIO
(b)(6)@treasury.gov		Contractor	Information Systems	CIO
(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
(b)(6)@treasury.gov	(b)(6)	Contractor	Information Systems	CIO
(b)(6)@treasury.gov	N/A	Contractor	Information Systems	CIO
(b)(6)@treasury.gov		Contractor	Information Systems	CIO
(b)(6)@treasury.gov		Contractor	Information Systems	CIO
(b)(6)@treasury.gov		Customer Support	Information Systems	CIO
(b)(6)@treasury.gov		Customer Support Analyst	Information Systems	CIO
(b)(6)@treasury.gov		Customer Support Analyst	Information Systems	CIO
(b)(6)@treasury.gov	(b)(6)	Data Center Operation Manager	Information Systems	CIO
(b)(6)@treasury.gov		Director of Enterprise Engineering	Information Systems	CIO
(b)(6)@treasury.gov		Director of Financial Systems Technology	Information Systems	CIO
(b)(6)@treasury.gov		Director, Technology Discovery and Integration	Information Systems	CIO
(b)(6)@treasury.gov		Enterprise Architect	Information Systems	CIO
(b)(6)@treasury.gov		Enterprise Architect	Information Systems	CIO
(b)(6)@treasury.gov		Financial Analyst	Information Systems	CIO
(b)(6)@treasury.gov		Financial Manager	Information Systems	CIO
(b)(6)@treasury.gov		GSOC	Information Systems	CIO
(b)(6)@treasury.gov	(b)(6)	GSOC	Information Systems	CIO
(b)(6)@treasury.gov		GSOC	Information Systems	CIO
(b)(6)@treasury.gov		GSOC	Information Systems	CIO
(b)(6)@treasury.gov	N/A	HSPD-12 Project Management	Information Systems	CIO
(b)(6)@treasury.gov		Information Technology Specialist	Information Systems	CIO
(b)(6)@treasury.gov	(b)(6)	IT Specialist	Information Systems	CIO
(b)(6)@treasury.gov		IT Specialist	Information Systems	CIO
(b)(6)@treasury.gov		IT Specialist	Information Systems	CIO
(b)(6)@treasury.gov		IT Specialist	Information Systems	CIO
(b)(6)@treasury.gov		IT Specialist	Information Systems	CIO
(b)(6)@treasury.gov		IT Specialist	Information Systems	CIO
(b)(6)@treasury.gov		IT Specialist	Information Systems	CIO
(b)(6)@treasury.gov		IT Specialist, ICAM	Information Systems	CIO
(b)(6)@treasury.gov	(b)(6)	IT Specialist, Information Security	Information Systems	CIO
(b)(6)@treasury.gov

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Records/Information - Obtained
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
February 1, 2021	February 2, 2021	875 15th Street, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C), Investigator, Office of Counterintelligence, Phone: (b) (6), (b) (7)(C)		(b) (6), (b) (7)(C), Senior Special Agent

On February 1, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) received Treasury Help Desk tickets from Office of Counterintelligence's (b) (6), (b) (7)(C). The help desk tickets include information concerning the breach, details regarding Treasury's Government Security Operations Center's (GSOC) response to the computer intrusion, and other associated details (Attachments 1 - 3).

Attachments:
1. 22440_As of 1 Feb 2021.pdf
2. 22445_DO_As of 1 Feb 2021.pdf
3. 22446_OFAC_As of 1 Feb 2021.pdf

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Witness
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
December 14, 2020	December 14, 2020	875 15th Street, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) (b) (6), (b) (7)(C) Information Technology, Treasury Office of Inspector General, (b) (6), (b) (7)(C), (b) (6), (b) (7)(C)		(b) (6), (b) (7)(C), Senior Special Agent

On December 14, 2020, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C) regarding the suspected intrusion of Treasury information systems, as reported publicly by news organizations on or about December 13, 2020. (b) (6), (b) (7)(C) Information Technology (IT) Department for the Treasury Office of Inspector General's Office of Management. (b) (6), (b) (7)(C) provided the following information in regards to the Treasury IG's network.

TIG ceased using SolarWinds about four years ago. It was discontinued because it was, as (b) (6), (b) (7)(C) said, expensive and overkill for what TIG needed. The IT Department has SolarWinds Toolset v.10.10.208 as well as Workspace Studio on a laptop. Out of an abundance of caution, the IT Department would be turning off the applications on the morning of December 14, 2020. The aforementioned SolarWinds toolset is not one of the applications reportedly used in the computer intrusions.

(b)(7)(E)

TIG's IT Department is in the process of implementing the Department of Homeland Security's (DHS) Continuous Diagnostics and Monitoring (CDM) program. (b) (6), (b) (7)(C) added that not all of the requirements from CDM have been fully implemented, but the IT department continues work towards fulfilling the requirements. The CDM is a means in which TIG provides data, like logs and other computer aggregated information, to DHS's Cybersecurity and Infrastructure Security Agency (CISA).

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

MEMORANDUM OF ACTIVITY

Case Number:	Subject of Activity (*Brief Description*):	Date of Activity:
CYBER-21-0019-I	(b) (6), (b) (7)(C)	December 14, 2020

On or about May, 2020, a (b)(7)(E) was made of the TIG network. The purpose of the scan was to identify all privileged accounts. A privileged user is one who is able to perform functions ordinary users are not authorized to conduct. Some stale, privileged accounts were identified during the scan and subsequently disabled. An example of a stale, privileged account is a vendor who installed a program on TIG's systems, needed the privileged account to conduct the work, but is no longer actively performing the same task.

(b) (6), (b) (7)(C) wants to remove all privileged accounts no longer in active use but doing so could create unintended consequences (b)(7)(E)

(b)(7)(E)

The IT Department attempted to (b)(7)(E) on December 14, 2020, but the temporary license appears to have expired, thus the scan could not be initiated.

There is one privileged account, (b)(7)(E) which is granted access into the TIG network. The (b)(7)(E) is used by Treasury to manage TIG's phone system. On December 14, 2020, Mr. (b) (6), (b) (7)(C) was able to confirm that no other entities, aside from Treasury's privileged (b)(7)(E) are able to gain authorized access to TIG's network.

In addition to (b)(7)(E), TIG IT uses (b)(7)(E)

(b)(7)(E)

The web based applications HRConnect, Integrated Talent Management System (ITM), and WebTA do not have direct access to the TIG network. They are accessed via a web browser but there are no connections to the TIG network, other than the normal web traffic. The emails generated by the aforementioned systems are not generated by TIG's mail servers. Emails are generated by the application itself and sent to a TIG email address. For example, an ITM notification is sent from "ITM_SYSTEMS_ADMINISTRATOR@TREASURY.NS2CLOUD.COM" stating a user

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

has outstanding training requirements. The email is sent to ITM participants at their TIG email address.

TIG IT has conducted network vulnerability assessments in the past. They have solicited assistance from Office of Audit's penetration testers. (b) (6), (b) (7)(C) has also sought out external agencies to conduct more thorough, in-depth vulnerability assessments.

(b)(7)(E)

Finally, (b) (6), (b) (7)(C) was formally notified of the computer intrusion via email at about 0100 hours on December 14, 2020. The message referenced the exploitation of SolarWinds Orion products versions 2019.4 through 2020.2.1 HF1 (Attachment 1).

Attachments:
1. Critical Incident Alert Email Notification

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

From: Luttrell, Sally
To: (b) (6), (b) (7)(C); (b) (6), (b) (7)(C)
Cc: McDowell, Sean A.
Subject: FW: ****CRITICAL ACTION ALERT from OCIO Cyber**** - Executive Directive 21-01 Mitigate SolarWinds Orion Code Compromise
Date: Monday, December 14, 2020 8:35:06 AM
Importance: High

FYI

Sally Luttrell
Assistant Inspector General for Investigations
US Department of the Treasury
Office of Inspector General
Office of Investigations
(b) (6), (b) (7)(C)
875 15th ST NW
Washington, DC 20005

From: Lawrence, Jeffrey
Sent: Monday, December 14, 2020 8:34 AM
To: Delmar, Richard K. (b) (6), (b) (7)(C); Luttrell, Sally (b) (6), (b) (7)(C); Harker, Deborah L. (b) (6), (b) (7)(C); (b) (6), (b) (7)(C) (b) (6), (b) (7)(C)
Subject: FW: ****CRITICAL ACTION ALERT from OCIO Cyber**** - Executive Directive 21-01 Mitigate SolarWinds Orion Code Compromise
Importance: High

All,

(b) (6), (b) (7)(C) got this at 1 am last night.

Jeffrey Lawrence
Assistant Inspector General for Management
U.S. Department of the Treasury
Office of Inspector General
875 15th Street, N.W.
Washington, D.C. 20005
Office Phone: (b) (6), (b) (7)(C)

From: (b) (6), (b) (7)(C)
Sent: Monday, December 14, 2020 8:30 AM
To: Lawrence, Jeffrey (b) (6), (b) (7)(C)
Subject: FW: ****CRITICAL ACTION ALERT from OCIO Cyber**** - Executive Directive 21-01 Mitigate SolarWinds Orion Code Compromise

Importance: High

From: CyberRisk@treasury.gov <CyberRisk@treasury.gov>
Sent: Monday, December 14, 2020 1:36 AM
To: CyberRisk@treasury.gov
Cc: (b)(6)@treasury.gov; Tony.arcadi@Treasury.gov; TreasuryCyberPerformance@treasury.gov
Subject: ****CRITICAL ACTION ALERT from OCIO Cyber**** - Executive Directive 21-01 Mitigate SolarWinds Orion Code Compromise
Importance: High

This message was sent securely using ZixCorp.

Bureau CISOs,

SolarWinds Orion products (**versions 2019.4 through 2020.2.1 HF1**) are currently being exploited by state-sponsored cyber actors. The affected products presents an attack vector allowing malicious cyber actors to gain access to network traffic management systems and subsequently move laterally to other systems. OCIO Cyber is requesting all Bureaus to take immediate and priority actions below per Executive Directive 21-01.

By **11:00AM Monday, December 14, 2020**, all Bureaus are required to take the following actions:

(b)(7)(E)

(b)(7)(E)

For questions, comments, or concerns, please email TreasuryCyberRisk@treasury.gov.

Thank you in advance for your support in completing these actions.
Enterprise Cyber Risk Management
Office of the Associate CIO, Cybersecurity
U.S. Department of the Treasury

This message was secured by ZixCorp(R). CAUTION: This email originated from outside of the organization. Please do not click any links or open attachments unless you recognize the sender and know the content is safe. Contact OM-IT if in doubt. Thank you.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Records/Information - Obtained
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
May 13, 2021	May 27, 2021	875 15th Street, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) [redacted] Office of CIO (b) (6), (b) (7)(C) [redacted]		(b) (6), (b) (7)(C) [redacted], Senior Special Agent

On May 13, 2021, Department of Treasury, Office of Inspector General (TIG) Senior Special Agent (b) (6), (b) (7)(C) [redacted] received Mandiant's report entitled Intrusion Investigation Report (Attachment 1). The file was provided to TIG by Treasury's (b) (6), (b) (7)(C) [redacted]. The report includes activities performed by FireEye Mandiant while they conducted incident response activities on behalf of the U.S. Treasury.

Attachments:
1. Intrusion Investigation Report

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Records/Information - Obtained
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
June 3, 2021	June 7, 2021	875 15th Street, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) Office of CIO (b) (6), (b) (7)(C)		(b) (6), (b) (7)(C) Senior Special Agent

On June 3, 2021, Department of Treasury, Office of Inspector General (TIG) Senior Special Agent (b) (6), (b) (7)(C) received four Mandiant status update reports from Treasury's (b) (6), (b) (7)(C) (Attachments 1 - 4). The reports include sections detailing activities Mandiant conducted and Mandiant's plans for the next reporting period. The last update report, ending April 6, 2021, states Mandiant has completed all requests.

Attachments:
1. 20210316 - MFR20-932 IR Status Update - 03-16-21.pdf
2. 20210323 - MFR20-932 IR Status Update - 03-22-21.pdf
3. 20210331 - MFR20-932 IR Status Update - 03-30-21.pdf
4. 20210407 - MFR20-932 IR Status Update - 04-06-21.pdf

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Records/Information - Obtained
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
April 23, 2021	April 26, 2021	875 15th Street, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) [redacted] Office of CIO (b) (6), (b) (7)(C) [redacted]		(b) (6), (b) (7)(C) [redacted], Senior Special Agent

On April 23, 2021, Department of Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) [redacted] received Microsoft's Detection and Response Team (DART) report entitled DAYTONABRONZE_v2_Outbrief.pptx (Attachment 1). The file was provided to TIG by Treasury's (b) (6), (b) (7)(C) [redacted]. The report is Microsoft's findings related to the intrusion and compromise of the Treasury network and its systems.

Attachments:
1. DAYTONABRONZE_v2_Outbrief.pptx

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	Interview - Victim
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
January 13, 2021	January 13, 2021	875 15th Street NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
(b) (6), (b) (7)(C) IT Specialist (b) (6), (b) (7)(C)		(b) (6), (b) (7)(C), Senior Special Agent (b) (6), (b) (7)(C) Senior Special Agent

On January 13, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agents (SSA) (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) interviewed (b) (6), (b) (7)(C) Information Technology Specialist, regarding the compromise of his government email address (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) provided the following information during the interview.

(b) (6), (b) (7)(C) is a (b) (6), (b) (7)(C) Treasury employee. He works for the System Engineering Group, which is headed by (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) is an engineer who designs, deploys, and configures information technology systems and resources.

About one or two weeks prior to December 25, 2020, Microsoft Corporation contacted the United States Treasury and informed the department it had observed anomalous activity regarding (b)(7)(E)

(b)(7)(E)

(b)(7)(E) The compromise of (b)(7)(E) indicated someone had gained access to Treasury's internal network. In response to the suspected compromise, Microsoft's DART Team is conducting an investigation and is expected to provide Treasury with a report of their findings.

On July 6, 2020, the SolarWinds global administrator account went to the Microsoft Azure portal and modified the Secure Mail application. This activity is presumed to have been done by an adversary. Modification of Secure Mail potentially allowed access to all email addresses ending in "treasury.gov". (b) (6), (b) (7)(C) however, did not know what was targeted in Secure Mail and what, if anything, had been obtained from Secure Mail. The intruder's access to Secure Mail continued to October 12,

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

2020, when a change in the system appears to have caused the inadvertent denial of access to Secure Mail.

In October, 2020, the anomalous (b)(7)(E) activity was first observed. (b)(7)(E) (b)(7)(E) (b)(7)(E) . In speaking with Microsoft, (b) (6), (b) (7)(C) understands the (b)(7)(E) (b)(7)(E) and the user's login activity is coming from within the organization's network. (b) (6), (b) (7)(C) (b)(7)(E) on data from January 13, 2020 thru January 11, 2021. (b) (6), (b) (7)(C) identified six accounts with the known code number. These include the following:

- (b) (6), (b) (7)(C)

Four other compromised accounts were not associated to the (b)(7)(E) . (b) (6), (b) (7)(C) contacted Microsoft to determine how these accounts were identified as compromised. Microsoft did not provide technical details to explain their conclusion. They advised they have other data sources which indicated the compromise. These four include the following:

- (b) (6), (b) (7)(C)

All of the compromised accounts were regular user accounts. None were privileged.

(b) (6), (b) (7)(C) said that Active Directory (AD) includes a description of all users and their positions. (b)(7)(E)

(b)(7)(E)

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

MEMORANDUM OF ACTIVITY

Case Number:	Subject of Activity (*Brief Description*):	Date of Activity:
CYBER-21-0019-I	(b) (6), (b) (7)(C)	January 13, 2021

(b)(6); (b)(7)(C); (b)(7)(E)

(b) (6), (b) (7)(C) has an old LinkedIn account and had a Facebook account before he deleted it four years ago. Neither have links to his Treasury email account or information.

(b) (6), (b) (7)(C) also provided a PDF report, from Microsoft, which is entitled "Cust_IOC_treas.pdf" (Attachment 1). The PDF includes a chronological breakdown of events, a list of IPs used in the (b)(7)(E) and a list of affected Treasury accounts.

In addition, (b) (6), (b) (7)(C) also provided an Excel spreadsheet entitled (b)(7)(E) From-1_13_2020__To-1_11_2021.xlsx" (Attachment 2). (b) (6), (b) (7)(C) generated the spreadsheet when he ran the (b)(7)(E)

Attachments
1. Customer IOC PDF
2. (b)(7)(E) Spreadsheet

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

IOC's Prepared for Treasury:

Anomalous Activity Characterized:

(b)(7)(E)

(b)(7)(E) Application Modification Timeline (2020/07/06):

(b)(7)(E)

Earliest Graph Abuse Timeline (2020/09/10 – 2020/10/08):

(b)(7)(E)

Earliest Azure Activity Directory Abuse (2020/08/10):

(b)(7)(E)

(b)(7)(E Authentication Timeline (2020/10/12 – 2020/11/05):

The following indicators are reflective of (b)(7)(E) .

(b)(7)(E)

(b)(7)(E)

Affected Accounts:

(b)(6); (b)(7)(E)

MEMORANDUM OF ACTIVITY

Case Number:	Reporting Office:	Type of Activity:
CYBER-21-0019-I	Investigations	LEO Activity - Record/Information Review
Date of Activity:	**Date Report Drafted:**	**Location of Activity:**
August 24, 2021	August 26, 2021	875 15th Street, NW, Washington DC
Subject of Activity:		**Activity Conducted By (Name(s) and Title(s)):**
Treasury Departmental Policy		(b) (6), (b) (7)(C), Senior Special Agent

On August 24, 2021, Department of the Treasury, Office of Inspector General (TIG) Senior Special Agent (SSA) (b) (6), (b) (7)(C) received Treasury's cybersecurity and incident response plan from (b) (6), (b) (7)(C). (b) (6), (b) (7)(C) is an (b) (6), (b) (7)(C) with the Government Security Operations Center. The plan is entitled Departmental Incident Response Plan, version 1.3, dated and last revised October 10, 2018 (Attachment 1). According to (b) (6), (b) (7)(C) the policy drives incident response activities. A review of the plan identified several points of interest, to include the following.

The incident response (IR) plan applies to Department of Treasury and Treasury bureaus. All Treasury bureaus have IR procedures and Computer Security Incident Response Teams (CSIRTs). The IR plans at the bureau level are customized to the bureau's particular needs and structure.

Treasury's overarching IR plan identifies the Treasury CIO as the authority to take or direct action in response to an information technology security incident or vulnerability. The Treasury CISO oversees the Department's cyber security posture, capabilities, and policy.

The Government Security Operations Center (GSOC) serves as the Department's primary IR center, and single point of contact and liaison for US-CERT, which is a component of Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. GSOC oversees all IR activities and provides support to all bureaus. The GSOC escalates incident reports to Treasury leadership.

The bureau CSIRCs serve as liaison to the GSOC and also oversee IR activities at the bureau level.

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

The policy also identifies the incident response process. It is an iterative approach moving from and between the following phases:

- preparation
- detection and analysis
- containment, eradication, and recovery
- post-incident activity

GSOC is to have capabilities to conduct and analyze host-based artifacts, malware analysis, log analysis, and more. They are to have mechanisms which can provide surge support in the event of a serious security incident.

Bureaus are required to report cyber incidents, like breaches, to GSOC and GSOC passes it to US-CERT. Bureaus are not to report directly to US-CERT.

Finally, at the conclusion of an incident of particular severity, the bureau or GSOC must complete an after action report to facilitate lessons learned.

Attachments:
1. Departmental Incident Response Plan v.1.3_10-10-18.pdf

This report contains sensitive law enforcement material and is the property of the Office of Inspector General. It may not be copied or reproduced without written permission from the Office of Inspector General. This report is FOR OFFICIAL USE ONLY. Its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



Department of the Treasury

OCIO – Cybersecurity

Departmental Incident Response Plan

10/10/2018

Version: 1.3

~~This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Questions about this plan or an incident affecting Treasury should be directed to the GSOC at:
soc@gsoc.treas.gov or (202)927-9777

Revision History

Version	Date	Description
1.0	9/15/16	Initial release
1.1	3/15/17	Updated to address US-CERT guidelines for 4/1/17, OMB M-17-12, and OMB M-17-05
1.2	9/15/17	Updated to incorporate Recover Plan elements as described in NIST SP 800-184 and add Appendix on Major Incident reporting
1.3	10/10/18	Updated to incorporate NIST guidance clarifying the establishment of information sharing rules; and NIST guidance for producing and publishing effective threat indicators.

Table of Contents

1. EXECUTIVE SUMMARY 5
1.1 INTRODUCTION 5
1.2 PURPOSE 5
1.3 SCOPE 5
1.4 AUTHORITY ESTABLISHMENT 5
2. ROLES AND RESPONSIBILITIES 6
3. DEFINITIONS 9
4. INCIDENT RESPONSE PROCESS 11
4.1 PREPARATION 11
4.2 DETECTION, ANALYSIS, AND REPORTING 13
4.2.1 DETECTION 14
4.2.2 ANALYSIS 15
4.2.2.1 PII IMPACT IDENTIFICATION 16
4.2.2.2 BREACH RISK/HARM ASSESSMENT 16
4.2.3 REPORTING AND ESCALATION 19
4.2.3.1 TREASURY INCIDENT SEVERITY SCHEMA 21
4.2.3.2 TREASURY INCIDENT STAKEHOLDER NOTIFICATION MATRIX 24
4.2.3.3 MAJOR AND SIGNIFICANT INCIDENTS 25
4.3 CONTAINMENT, ERADICATION, MITIGATION, AND RECOVERY 26
4.3.1 SYSTEM SHUTDOWN 27
4.3.2 SYSTEM RECOVERY 27
4.3.3 BREACHES 27
4.3.3.1 BREACHES AFFECTING TREASURY PERSONNEL OR CONTRACTORS 28
4.3.3.2 BREACH NOTIFICATION 28
4.3.3.3 BREACH REMEDIATION 29
4.4 POST-INCIDENT ACTIVITY 29
4.4.1 POST-INCIDENT ANALYSIS 29
4.4.2 REPORTING AND METRICS 30
5. ACRONYMS 30
APPENDIX 32
Appendix A - Impact Classification Descriptions by US-CERT 32

Appendix B – Observed Activity Definitions 34
Appendix C – Incident Attributes Defined by US-CERT 35
Appendix D – Example Incident Reporting Interpretations 37
Appendix E – FAQs for Major Incidents 41

1. EXECUTIVE SUMMARY

1.1 INTRODUCTION

The Department of the Treasury faces a wide array of threats from adversaries with varying levels of resources and technical prowess. The Department also must protect against unauthorized internal and external disclosures of information. The Department must remain vigilant and must be prepared to respond to these threats to our systems and/or information.

1.2 PURPOSE

In order to improve the rapidity and agility with which the Department responds to suspected and confirmed incidents, this plan establishes Departmental incident response (IR) procedures, streamlining efforts across all bureaus. An important element of this plan is centralized incident response reporting and tracking, which promotes efficient threat analysis, correlation and mitigation across all bureaus. The plan establishes common reporting criteria as directed by the Office of Management and Budget (OMB). It will also outline the IR coordination procedures for Treasury, its bureaus, and how Treasury coordinates with the Department of Homeland Security (DHS).

1.3 SCOPE

The Departmental Incident Response Plan (IRP) applies to the Department of the Treasury and all Treasury bureaus. Consistent with Treasury cybersecurity and privacy policy, requirements established herein apply to all Treasury information and information systems, including Treasury contractor or subcontractor systems (defined as systems operated for or on behalf of bureaus by a contractor, subcontractor, or other organization, whether owned by the contractor/subcontractor and operated for Treasury or owned by Treasury and operated by one or more contractors/subcontractors.)

All Treasury bureaus have established extensive IR procedures and Computer Security Incident Response Teams (CSIRTs) in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and industry best practices. These IR plans have been customized to fit specific bureau threat landscapes. The Departmental IRP provides enterprise-wide guidance on necessary steps that must be taken by, and in coordination with, Treasury and all bureaus upon the discovery of an incident. This plan is not meant to replace bureau IRPs, nor is it intended to be a comprehensive guide for responding to individual incidents.

1.4 AUTHORITY ESTABLISHMENT

The Departmental IRP is enforced by: (1) the Department of the Treasury Office of the Chief Information Officer (OCIO) under the authority of the National Security Council (NSC), OMB, and DHS as outlined in OMB Memoranda M-17-05, M-16-03, and M-15-01, and (2) the Treasury Senior Official for Privacy as required by OMB M-17-12. This plan is also authorized under OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources; Presidential Decision Directive 63 (PDD-63), *Critical Infrastructure Protection* and OMB M-16-03, which outlines guidelines for formalizing the process for federal agencies to request and receive on-site technical assistance from DHS. IR procedures for addressing incidents concerning a breach of personally identifiable information (PII) are established in

accordance with OMB-M-17-12 (Preparing for and Responding to a Breach of Personally Identifiable Information).

The Department has also outlined, in Treasury Directive Publication (TD P) 85-01, IR program requirements tasking bureau Chief Information Officers (CIOs) to maintain proper IR programs to facilitate bureau capabilities for responding to, investigating, mitigating, and reporting incidents involving bureau resources and infrastructure. Furthermore, Treasury Directive (TD) 85-03 establishes the authorities of the Departmental CIO to coordinate with bureau officials to take appropriate action in the event of an actual, suspected, or threatened information technology (IT) security incident or a significant IT vulnerability. TD 25-08, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, establishes Treasury and its bureaus' responsibilities when responding to a breach (involving PII)

The IRP leverages these authorities to provide complementary and supplemental procedural requirements for the Department and its bureaus.

2. ROLES AND RESPONSIBILITIES

The Personally Identifiable Information Risk Management Group (PIIRMG)

- Comprised of: The SAOP; the CIO or the CIO's designee; the Senior Agency Information Security Officer; legal counsel; a representative from the Office of Legislative Affairs; and a representative from the Office of Public Affairs.
- Assist the bureaus in addressing certain extraordinary PII breaches as discussed in TD-25-08.
- Consult with budget, procurement, human resources, law enforcement, intelligence, physical security and other personnel as needed to address issues related to a breach for which it is providing assistance.

Treasury Senior Agency Official for Privacy (SAOP)

- Oversee the Departmental response to breaches involving personally identifiable information.
- Serve as the chair of Treasury's PIIRMG (per TD-25-08).
- Notify the Secretary and Deputy Secretary of the occurrence of a breach, as necessary.
- Serve as focal point with the Office of Management and Budget and Congress on all matters pertaining to a breach and coordinate mitigation actions with the respective Inspectors General Offices as appropriate.

Treasury Deputy Assistant Secretary for Privacy, Transparency, & Records (DAS PTR)

- Provide the day-to-day operational support for the PII Breach Response Management Group (PIIRMG).

- Provide critical review and analysis of issues and problems impacting mitigation of breaches and privacy protection activities within Treasury.
- Notifies the PIIRMG of any breach in the event that the Bureau Head or designee informs the DASPTR that a breach has ramifications beyond the affected bureau or cannot be adequately addressed by the affected bureau alone.
- Identifies and provides applicable privacy compliance documentation to the PIIRMG, the SAOP, and bureaus as necessary to conduct a breach risk assessment.

Treasury CIO

- Oversee the Department's Information Technology programs.
- Empower the Department-level IT and cyber security teams to respond to security incidents.
- Serve as the chair of the Treasury CIO Council.
- Exercise Treasury authority to take or direct necessary and appropriate actions in response to an actual, suspected, or threatened IT security incident or significant IT vulnerability.

Treasury CISO

- Oversee the Department's cyber security posture, capabilities, and policy to ensure the Department is working to protect, detect, identify, respond and recover from cyber incidents.
- Serve as a co-chair of the Treasury Cybersecurity Board.

Treasury Government Security Operations Center (GSOC)

- Serve as the Department's primary IR center and single point of contact for and liaison to the DHS United States Computer Emergency Readiness Team (US-CERT).
- Oversee all Departmental IR activities and provide investigative and mitigation support to all bureaus.
- Facilitate indicator and tactical information exchange about cyber incidents amongst appropriate Department stakeholders.
- Identify major incidents.
- Escalate incident reports to Treasury leadership and engage key Departmental stakeholders in the IR process, as appropriate.
- Send all reports of breaches (involving electronic and non-electronic PII) to the DAS-PTR or his/her representative.

Bureau CIO

- Empower bureau CSIRC to investigate and respond to incidents.
- Ensure internal bureau response execution, including engagement of bureau privacy personnel with respect to breaches and appropriate escalation to senior bureau officials, is performed.
- Participate in the Treasury CIO Council.

Bureau CISO

- Ensure the bureau adheres to Treasury policy, follows best practices, and is adequately prepared to prevent, detect, identify, respond, and recover from cyber security incidents.
- Serve as a member of the Treasury Cybersecurity Board.

Bureau CSIRCs

- Serve as primary coordination point for IR within the bureau.
- Oversee IR activities at the bureau level.
- Serve as the liaison to the GSOC for all communications and follow up activities in response to an incident.

Bureau Privacy Offices

- Work with the Bureau OCIO on all response activities for breaches to ensure completion of actions required by policy.
- Inform and coordinate with DASPTR and the PIIRMG on breaches as necessary and required by policy.
- Ensure that all breaches (involving electronic and non-electronic PII) are reported to GSOC and appropriate actions are taken to investigate and respond to both types of breaches.
- Ensure the relevant Inspector General, the Office of Counterintelligence, and other applicable regulatory agencies are notified in the event of a breach.

Office of Intelligence and Analysis, Office of Counterintelligence (OIA/OCI)

- Investigate all security incidents that may relate to a foreign intelligence threat to the Department.
- Ascertain whether there are indications of an insider threat and, if so, assist in mitigating the threat.
- Serve as the Department's liaison to the Intelligence Community.

Office of Legislative Affairs

- Facilitate Congressional notification for incidents when required, such as for major incidents.
- Coordinate with bureau Legislative/Congressional Affairs teams.

Office of Public Affairs

- Coordinate press releases and responses to media inquiries.
- Coordinate with bureau public affairs teams.

Office of Security Programs (OSP)

- Oversee response to incidents affecting classified data or information.

Office of Critical Infrastructure Protection and Compliance Policy (OCIP)

- Coordinate information sharing or IR that has impact to or involves the financial sector.
- Facilitate information sharing of any indicators or other information from Departmental cyber attacks with the financial sector.

Office of the Inspector General (OIG)

- Provide law enforcement support for applicable security investigations at all non-IRS bureaus, if appropriate authority does not already exist at the bureau.
- Serve as a liaison to engage additional law enforcement support, such as the FBI.

Treasury Inspector General for Tax Administration (TIGTA)

- Provide law enforcement and investigative support for security investigations at the IRS.
- Serve as a liaison to engage additional law enforcement support, such as the FBI.

Treasury Cybersecurity Board (TCB)

- As a council formed of all Treasury bureau CISOs, direct policy updates and coordinated action when multiple bureaus are impacted by a security event.

Treasury CIO Council (CIOC)

- As a council formed of all Treasury bureau CIOs, direct policy updates and coordinated response action when multiple bureaus are impacted by a security event.

3. DEFINITIONS

Table 1 – Incident, Breach, and Event definitions

Activity Type	Definition
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) a person accesses or potentially accesses personally identifiable information for an unauthorized purpose (i.e., a purpose unrelated to their official duties/functions). INFORMATIONAL: A breach is a type of incident.
Incident	An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Major incident[1]	Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. A breach constitutes a major incident when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a "major incident."
Significant cyber incident[2]	A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. *NOTE: All major incidents are also deemed significant cyber incidents. However, only when a breach of PII that constitutes a "major incident" is the result of a cyber incident will it meet the definition of a "significant cyber incident" and trigger the coordination mechanisms outlined in PPD-41.*
Suspected incident	An occurrence or alert that is under investigation as a potential incident but has yet to be confirmed.
Suspected breach	An occurrence or alert that is under investigation as a potential breach but has yet to be confirmed.
Notable cyber event	Any deviation from the norm or observable occurrence in a network or system that could have led to a cyber incident but was otherwise mitigated and the source or threat vector poses an ongoing risk to the Department.
Cyber event	Any observable occurrence in a network or system that may indicate a cyber incident has occurred.

All confirmed or suspected cyber incidents and certain cyber events that involve PII are also "breaches" as that term is defined. All breaches are considered to be incidents. In the case where an incident is also a breach, it is important that bureaus also follow the breach guidance contained within this document. Incidents that are not breaches do not require application of the breach sections of this document.

[1] As defined by OMB in M-17-05.

[2] As defined in PPD-41

4. INCIDENT RESPONSE PROCESS

IR follows a four phase life cycle: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. During the incident investigation and response process, the process often is iterative, shifting between analysis and response actions as additional facts emerge. While the order may vary depending on the circumstances, all steps are important and cannot be skipped.

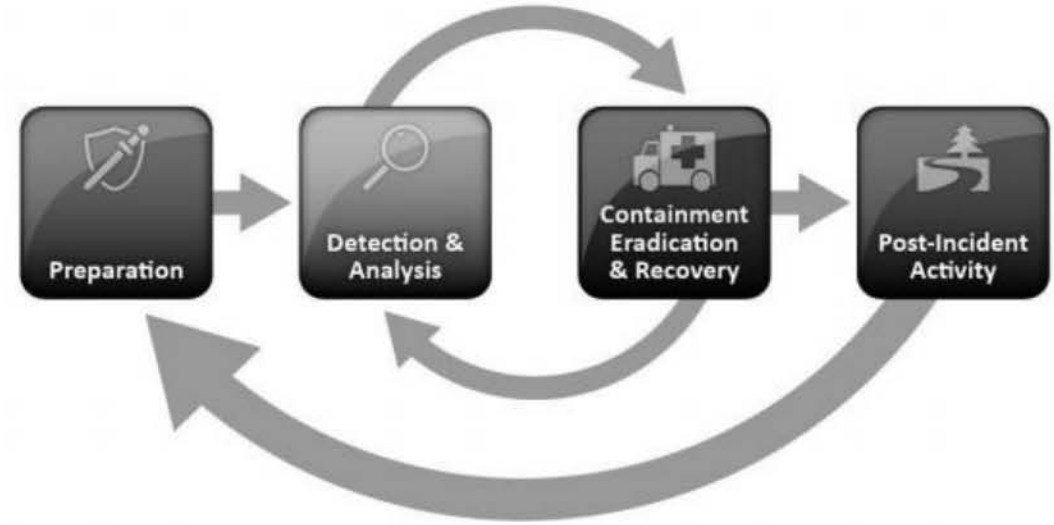


Figure 1 - Incident Response Life Cycle from NIST SP 800-61r2

4.1 PREPARATION

To be prepared for IR, bureau CIOs and Privacy Officers (or their designees) must:

- Implement detailed, centralized logging throughout their infrastructure.
- Ensure compliance with time stamp and time synchronization requirements stated in TD P 85-01.
- Deploy appropriate technologies to prevent, detect, identify, contain, respond to, and recover from security incidents.
- Ensure they have adequately trained personnel for IR activities.
- Create and maintain bureau-level IRPs and procedures for how to detect, analyze, report and escalate incidents and breaches.
- Create and maintain bureau or system-level recovery plans, either standalone or integrated in other documents such as Business Continuity Plans, to document and maintain specific strategies and decisions regarding how to implement and conduct business recovery procedures.
- Be prepared to search their environment for indicators of compromise (IOCs) as quickly as possible and in no more than 24 hours. IOCs can include network (i.e., IP or domain) or host (i.e., MD5 hash or filename) based indicators.
- Have at least the CISO and preferably additional security personnel cleared to at least the Secret level. If possible, obtain a TS/SCI clearance for key IR stakeholders, including the bureau privacy officer.

- Participate in Departmental IR exercises. Perform additional bureau- or system-level response or recovery exercises where appropriate.
- Ensure incident reporting and response staff has access to the TCSIRC portal.
- Facilitate relationships among key Bureau stakeholders in IR processes to prepare for rapid response, which may include but is not limited to:
    - CSIRC
    - CIO/CISO
    - System owners and operators
    - Privacy
    - Public affairs
    - Legislative affairs
    - Bureau senior leadership
    - Human resources
    - Legal counsel
    - Counterintelligence and Insider Threat Program
- Ensure bureau users are adequately trained to prevent and react to security events and incidents as appropriate.
- Ensure that the bureau has prepared in advance to take timely and appropriate countermeasures (e.g., identity monitoring, credit monitoring, and other related services) consistent with OMB Memorandum M-16-14, which, except under limited circumstances, requires the use of General Services Administration's (GSA) identity protection services (IPS) blanket purchase agreements (BPAs).
- Ensure bureau or system incident, breach response, and recovery plans are reviewed no less than annually, updated if necessary, and that the date of review is properly documented in the plan.

To be prepared for IR, the GSOC must:

- Identify points of contact for bureaus and Departmental organizations relevant for IR activities.
- Maintain capabilities for advanced analysis, including but not limited to host-based forensics, malware analysis, cyber threat intelligence, and log analysis and data mining. Whenever practical and relevant to IR activities, GSOC should also seek to enrich IOCs with further context and metadata.
- Have adequately trained personnel to analyze bureau reports and support bureau response efforts.
- Have a mechanism to provide surge support in the event of a serious security incident.
- Execute IRP exercises twice a year to promote Departmental preparedness for IR.
- Ensure the Departmental IRP is reviewed no less than annually, updated if necessary, and that the date of review is properly documented in the plan.
- Maintain designation as the primary POC for US-CERT for all cyber incidents.
- Ensure Treasury has a valid standing Federal Network Authorization to facilitate DHS on-site support when necessary.

- Maintain a centralized incident reporting mechanism and report repository.
- Maintain staff cleared up to the TS/SCI level.
- Be capable of meeting Trusted Internet Connection (TIC) 2.0 requirements for timely classified communications.

4.2 DETECTION, ANALYSIS, AND REPORTING

During the detection, analysis, and reporting process, an event/incident can be characterized as progressing through a series of states that describe the level of confidence that the issue in question is, in fact, an incident.

Incident State	Definition
Event occurred	The event took place
Event detected	The event was detected or discovered. This could be something like an alert from a security tool fired, a user submitted a report, a system administrator flagged something suspicious, etc. This is the catalyst event that triggers opening an investigation; however, not all detections will end up becoming investigations.
Event investigation opened	Appropriate staff determined the detected event was worth investigating and took action to begin gathering or analyzing information.
Suspected incident identified	The investigation reaches a point where (1) the bureau or GSOC has a reasonable suspicion an incident has occurred or (2) the event cannot be easily ruled out as a false positive or other non-incident in a timely fashion and therefore indicates an incident may have occurred or (3) the bureau has decided to execute a specific remediation action out of an abundance of caution (e.g., reimaging a possibly infected machine).
Incident confirmed	The evidence now confirms that an actual incident or breach has occurred.
Incident resolved	The mitigation and response actions and required data gathering, such as impact assessments, are complete.

Figure 2 - Incident States Definition

At a high level, the process flow between a bureau and the GSOC will look like the following during the detection, analysis, and reporting phase of an incident:

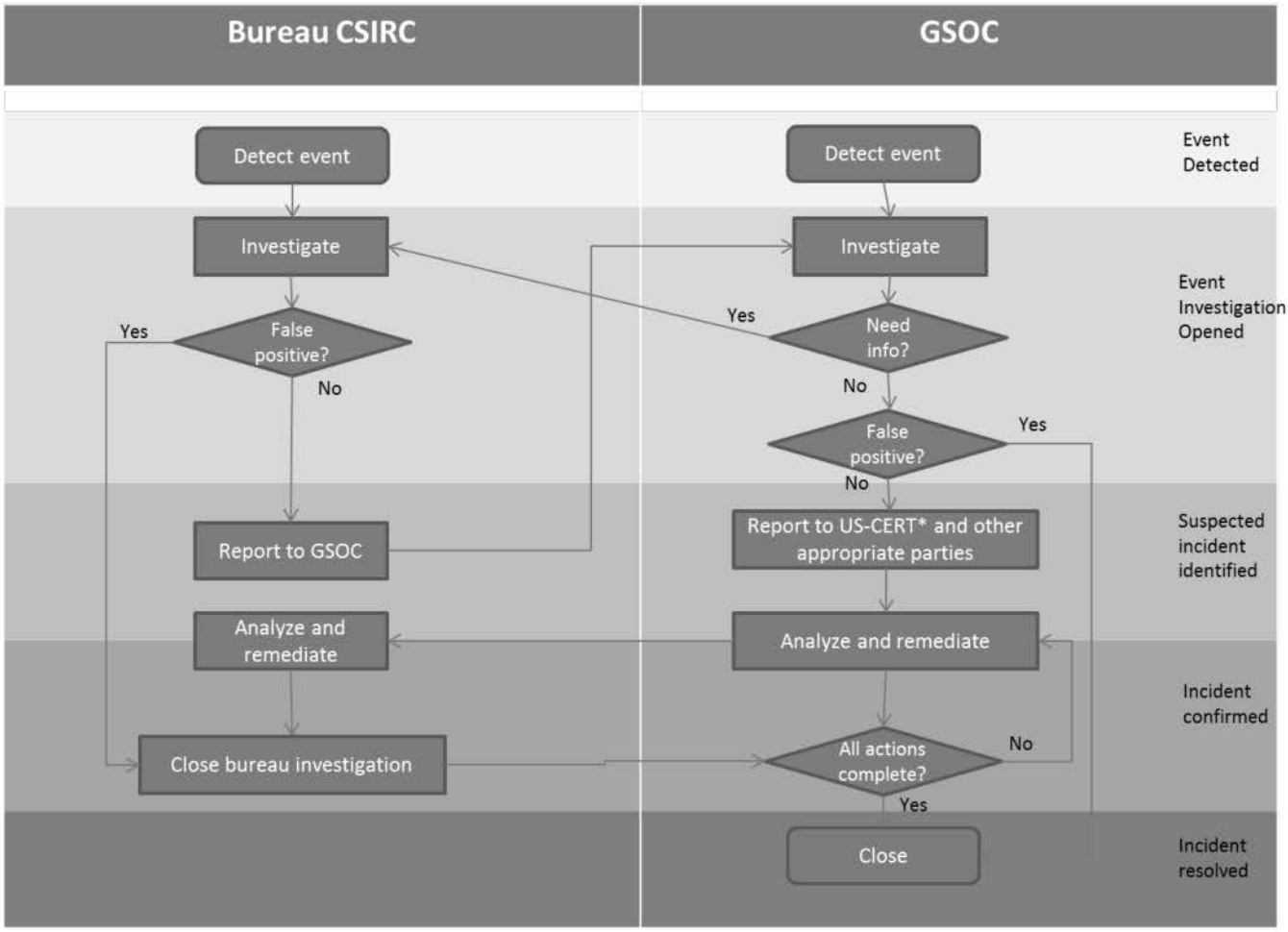


Figure 3 - Detect, Analyze, and Report Process Flow at Treasury

This diagram depicts an important distinction: the bureau and the GSOC may assess an event is a "suspected incident" at different times. As such:

- The bureau MUST report to GSOC as quickly as possible and in no more than one business day once they have identified what they believe to be a suspected incident.
- When a bureau submits a suspected incident to GSOC, GSOC will review the report and officially determine whether to classify the event as a suspected or confirmed incident. Once classified as such by GSOC, GSOC is responsible for reporting to US-CERT within one hour.
- If GSOC initiates an investigation into bureau traffic from their own detection, the GSOC may or may not need to get bureau concurrence before deeming it a suspected incident and reporting to US-CERT.

4.2.1 DETECTION

Incidents, breaches, and events may be detected by various means and by various groups, including at the bureau level by individual personnel, as well as by IT and security teams through different methods such as antivirus systems, firewalls, intrusion detection systems, system log review, observation by personnel, or by report from individuals outside the department.

At the Departmental level, GSOC detects incidents leveraging various security monitoring tools. GSOC also receives notifications and alerts from DHS/US-CERT and other external partners.

In most environments, the majority of security alerts are non-incidents or false positives and therefore never become reported incidents. The bureaus and GSOC are responsible for ensuring they have mechanisms to triage these various detection mechanisms to identify the most likely candidates for incidents.

4.2.2 ANALYSIS

After initial detection, the GSOC or the appropriate bureau personnel should investigate the report to determine if the report is truly an incident and to gather information to use for reporting and response activities. Furthermore, security personnel must gather information to prioritize incidents, breaches, and events to determine which items should get the quickest attention.

Throughout the investigative process, personnel must obtain and update the following required information and should try to obtain the optional information:

- [Required] Contact information for both the impacted and reporting organizations
- [Required] Description of what did or is suspected to have occurred, including impact
- [Required] Date/Time of occurrence, including time zone
- [Required] Date/Time of detection and identification, including time zone
- [Required] Associated System Name (as tracked in TFIMS)
- [Required] Physical system location(s) (e.g. Washington, DC, Los Angeles, CA)
- [Required] Prioritization factors (see Appendix A):
    - Functional impact
    - Information impact
    - Recoverability
- [Required] Mitigation actions taken or planned, if applicable
- [Required] Impact assessment (i.e., number of records and/or users affected)
- [Required if applicable] Data elements / information types involved (e.g., SSN, Name, Phone numbers, taxpayer information, medical/health information, financial information)
- [Required if applicable] Information regarding vulnerable populations involved (e.g., active duty military; government officials in sensitive positions, senior citizens, individuals with disabilities, confidential informants, witnesses, certain populations of immigrants, non-English speakers, and victims of certain crimes such as identity theft, child abuse, trafficking, domestic violence, or stalking)
- [Required] Observed Activity, if known (see Appendix B)
- [Optional] Related indicators (e.g. hostnames, domain names, network traffic characteristics, registry keys, X.509 certificates, MD5 file signatures)
- [Optional] Details describing any vulnerabilities involved (i.e., Common Vulnerabilities and Exposures (CVE) identifiers)
- [Optional] Source and Destination Internet Protocol (IP) address, port, and protocol
- [Optional] Operating System(s) affected

- [Optional] Mitigating factors (e.g. full disk encryption or two-factor authentication)
- [Optional] Device Function(s) (e.g. web server, domain controller, or workstation)
- [Optional] Sources, methods, or tools used to identify the incident (e.g. Intrusion Detection System or audit log analysis)

Analysis is often an ongoing process and bureaus should not hold up reporting due to an inability to provide complete information. GSOC can provide investigative assistance to bureaus upon bureau request including but not limited to: host forensics, network forensics, log analysis, malware analysis, and cyber threat intelligence. GSOC may also direct bureaus to provide information or artifacts for analysis, answer questions, or provide assessments or analysis of suspicious activity. Bureaus must acknowledge GSOC requests and respond in a timely fashion and within timeframes established for updates in later sections of this document.

4.2.2.1 PII IMPACT IDENTIFICATION

It is crucial at the initial analysis stage for the bureau help desk or CSIRC to identify whether the incident involves PII, including paper or oral disclosures (e.g., unauthorized disclosures to individuals who lack a need to know).

The term PII, as defined by OMB in Circular No. A-130 as, "*information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.*" This broadly-worded definition encompasses a great deal of information. Therefore, Treasury is required to perform an assessment to determine the risk that an individual can be identified based on the information itself or when the information is combined with other information that is linked or linkable to the individual. The bureau therefore must ensure front-line personnel have a full understanding of the breadth of the OMB definition of PII.

4.2.2.2 BREACH RISK/HARM ASSESSMENT

In order to prioritize PII breaches and determine whether additional countermeasures are appropriate, the bureau must assess the risk of harm associated with the breach. In the event of a suspected or confirmed breach, the bureau will assess all risks relevant to the breach, including risks to: (1) individuals potentially affected; (2) Treasury information systems; (3) Treasury programs and operations; (4) the Federal Government; and/or (5) national security. These risks are not mutually exclusive; a single breach (e.g., involving security clearance information) could affect an individual, Treasury systems and operations, the Federal Government and national security.

Bureaus may develop their own analysis system to ascertain thresholds relating to the number of individuals affected and the likelihood of risk/harm in the suspected or confirmed breach. In order to perform this analysis, the following must be evaluated and assessed:

1) The nature of the data elements subject to the breach.

Single Data Elements Containing PII. Certain data elements are particularly sensitive and may alone, under certain circumstances, present an increased risk of harm when they are linked or

linkable to the individual. These data elements include, but are not limited to, SSNs, passport numbers, driver's license numbers, state identification numbers, bank account numbers, passwords, and biometric identifiers.

Combining Data Elements Containing PII. Sometimes multiple pieces of information, none of which are particularly sensitive in isolation and would not present a risk of harm to the individual, may present an increased risk of harm to the individual when combined.

2) The nature of the PII subject to breach.

PII That May Subject an Individual to Embarrassment, Blackmail, or Emotional Distress. Assess whether the information involved is of a type that an individual would generally keep "private." Such "private information" may not present a risk of identity theft or other criminal conduct but may pose a risk of harm such as embarrassment, blackmail, or emotional distress. Examples include personnel or criminal information, personal debt and finances, medical conditions, treatment for mental health, pregnancy related information including pregnancy termination, sexual history or sexual orientation, adoption or surrogacy information, and immigration status.

PII That May Subject an Individual to Identity Theft or Other Financial Risk. A breach involving certain types of information may increase the possibility that the individual could become the victim of identity theft or other financial crime. This includes SSNs, bank account numbers, credit card numbers (especially when combined with the expiration date and three-digit code on the back), bank card pin numbers, passwords, or tax identification numbers.

PII That Cannot Be Changed. Some types of PII can be changed. When assessing risk, certain information can be modified (e.g., a credit card number) to reduce the risk of harm in the future if prompt action is taken. Special consideration is warranted, however, when a breach involves permanent biometric information including fingerprints, hand geometry, retina or iris scans, and DNA or other genetic information (considering both current and future uses).

3) Determine context by considering all relevant facts and circumstances regarding the breach and the PII involved in the Breach.

Context must be considered in assessing risk. This includes assessment of the purpose for which the PII was collected, maintained, and used so the situation can be fully understood and assessed. Contextual assessment is critical because the same information in different contexts can reveal more or less information about the potentially impacted individuals (e.g., the name of an individual on a list of personnel who attended a meeting on tax policy vs. a name of an individual on a request for an accommodation for a disability).

Context Includes an Assessment of the Vulnerabilities of Potentially Affected Individuals. Potentially vulnerable populations include, but are not limited to: children; active duty military; government officials in sensitive positions; senior citizens; individuals with disabilities; confidential informants; witnesses; certain populations of immigrants; non-English speakers; and victims of certain crimes such as identity theft, child abuse, trafficking, domestic violence, or stalking. This is not a comprehensive list and other populations may also be considered vulnerable.

4) Determine the likelihood that the breached PII is accessible to and usable by those with unauthorized access to it;

Identify All Security Tools Used to Protect the Data. Bureaus must consider on a case-by-case basis each of the security safeguards employed and take into account whether the type, value, or sensitivity of the information might motivate a malicious actor to put time and resources into overcoming those safeguards. This includes an analysis of all of the security features available in the format or media type involved, how long the PII was exposed, whether encryption was used, the likelihood that any encryption keys were exposed during the breach, whether PII was capable of and actually remotely wiped, and whether data masking, redaction, truncation, or anonymization were used (assuming the information underlying these techniques [e.g., redacted information available in the system to some but not all users] was not itself exposed during the breach).

Determine How Long the PII Was Exposed. Bureaus must also assess whether PII was exposed for an extended period of time in a manner that makes it more likely to have been accessible to unauthorized users (e.g., PII published to a bureau website for five minutes versus 2 days).

Assess Whether Evidence of Misuse Already Exists. Bureaus may also have access to evidence that the PII is already being misused (e.g., law enforcement indicates that the PII is already showing up on websites that sell stolen PII) or forensic or other analysis reveals that it was never accessed (e.g., a box of PII sat by an elevator for two days but 24 hour video cameras indicate that no one ever approached or opened the box).

5) Assess whether the intentional or unintentional nature of the breach can be determined;

Evidence of Intent to Target the Information or Device May Elevate Risk. After analyzing the considerations referenced above, the Bureau must assess whether evidence exists to determine whether the breach was intentional, unintentional, or whether the intent is unknown. If a breach was intentional, the Bureau should determine whether the information and/or the device itself was the target (e.g., a mobile phone or laptop) or whether the compromise of the information was incidental (e.g., an employee's car was stolen and there was an encrypted laptop containing PII in the trunk). Also the intent of the employee responsible for the PII disclosure should always be considered (i.e., are there any facts to suggest the employee disclosed the PII intentionally?).

Evidence of No Intent to Target the Information or Device May Still Reveal a High Risk. Though the risk of harm is typically higher with intentional breaches, the context of an unintentional breach may also reveal a high risk of harm (e.g., assume the laptop in the trunk of the stolen car referenced above was not encrypted or password protected and contained SSNs, tax and bank account information and law enforcement confirmed the information is already being posted on the internet).

Evidence That the PII Was Disclosed to a Known or Unknown Recipient. If disclosure was made to a trusted recipient who promptly notified the Bureau about the inadvertent disclosure this may be an indication of a low risk of harm to individuals, particularly when the recipient is another employee within the agency's IT network. The same may be true for trusted individuals outside the

Treasury's IT network. If analysis reveals that the PII is under control of a group or person who is either untrustworthy or known to exploit compromised information (e.g., which could include someone previously believed to be a trusted recipient who is acting suspiciously), the risk of harm to the individual is considerably higher.

6) Determine the capability of the bureau to mitigate the harm resulting from the Breach independently.

In the event of a high severity breach (e.g., a "Major Breach" as defined by OMB See Appendix F), Treasury may elect to assume responsibility for breach notification. The Assistant Secretary for Management, as Treasury's Senior Agency Official for Privacy (SAOP), in coordination with the Bureau breach response team, and, where appropriate, the Departmental Personally Identifiable Information Risk Management Group (PIIRMG), is responsible for advising the head of the agency on whether to take countermeasures (e.g., changing passwords; monitoring database for unusual activities), to offer guidance, or to provide services to individuals potentially affected by a breach. The GSOC or Bureau CIOs will determine whether the specific circumstances and type of PII potentially compromised by a breach require the involvement of other oversight entities.

The results of this analysis will also be used to determine whether breach notification or remediation is required (see Section 5.2 of this plan).

4.2.3 REPORTING AND ESCALATION

Bureaus are required to report to GSOC and GSOC to US-CERT as follows:

Table 2 - CSIRC and SOC Reporting Requirement

Activity Type	Bureau report to GSOC	GSOC report to US-CERT
Breach Incident Suspected incident Suspected breach	Required as quickly as possible and in no more than one business day from identification as a suspected or confirmed incident	Required within 1 hour of validating the event is a suspected or confirmed incident
Notable cyber event	Optional	Optional – if will help US-CERT protect others or if assistance is needed

Bureaus should conform to the following guidelines for reporting incidents to GSOC:

- Bureaus shall never report incidents directly to US-CERT.
- Bureaus must report to GSOC all applicable incidents and breaches within established timeframes and are encouraged to report additional notable cyber events for situational awareness.

- Bureaus must ensure that events do not remain in the "event investigation" phase too long. An event that cannot be ruled out as a non-incident within a reasonable amount of time should be considered a suspected incident and must be reported to GSOC.
- Bureaus must report as quickly as possible once they have enough information to report something has or is suspected to have occurred. Do not delay the reporting incidents while awaiting further details as this could result in higher risk to the system.
- While reporting incidents, the bureau CSIRC must use the standard reporting schema as established by GSOC.
- Bureaus should leverage the TCSIRC portal to submit, update, and manage incident reports if at all possible. When not possible, bureaus may update GSOC via email or phone and GSOC will enter the information into the TCSIRC portal.
- Bureaus must update incident reports as they continue their analysis or undertake mitigation actions, paying attention to escalation and update timeframes described later in this section.
- Bureaus must respond to additional requests for information from the Department regarding their incident investigation.
- Bureaus must inform the GSOC in advance of performing any external reporting, such as Congressional notifications, other government agency notifications, or press releases. Any such notifications must be coordinated with the Department before they occur. Furthermore, the bureau must report to the GSOC all details of the external notification, including:
    - The content of the notification
    - The date of the notification
    - The recipient(s) of and transmission mechanism for the notification
- Bureaus must inform the GSOC of any victim notifications as follows:
    - Routine victim notification must be reported to GSOC within a reasonable amount of time after the notification occurred. This only applies to situations where bureaus have a routine, periodic process to do notifications for small scale losses.
    - For any other victim notifications, including large scale, unusual, or situations otherwise deemed likely to generate leadership or external interest, bureaus must inform the GSOC in advance of performing victim notification.
    - Furthermore, the bureau must report to the GSOC all details of the external notification (without including PII beyond the incident number), including:
        - The basis for the notification
        - The content of the notification
        - The date of the notification
        - The transmission mechanism for the notification
        - Services offered to the victim, if any
- Bureaus must indicate once all required actions have been completed and the report is ready for closure.
- Bureaus must not include any classified information or unnecessary PII in the incident report.
- Bureaus must report indicators as they become available during an investigation.

GSOC is responsible for:

- Reviewing bureau incident reports, analyzing the available information, officially assessing the report as a confirmed or suspected incident and assigning it a Departmental severity level.
- Once assessed as a confirmed or suspected incident, sending appropriate reports to US-CERT, OMB, and Treasury leadership and offices.
- Engaging PTR for all confirmed or suspected breaches.
- Engaging Departmental Legislative and Public Affairs offices to ensure Congressional or public notification occurs when appropriate. Bureaus retain responsibility for internal escalation procedures as appropriate.
- Facilitating indicator and information sharing within the Department and with external stakeholders and partners. Before conducting information sharing activities, GSOC will:
    - Define the scope of information sharing activities by determining the types of information available to share and the circumstances under which sharing is permitted;
    - Identify approved recipients of threat information;
    - Describe requirements for redacting or sanitizing information that will be shared;
    - Clearly state whether source attribution is permitted; and
    - Apply handling designations that describe the recipient's obligations for protecting threat information.
- Determining if an incident meets the "major incident" definition.
- In the event of a cyber event or incident that has Departmental or multi-bureau implications, the GSOC will take actions to ensure all bureaus are aware, including:
    - Email notifications and reports
    - Conference calls
    - Classified (if necessary) and unclassified briefings
- In the event that an issue requires significant leadership attention, new or updated policy, or multi-bureau coordination, the GSOC will escalate to the Treasury CISO and CIO, who may convene the TCB or CIOC for awareness or action.

4.2.3.1 TREASURY INCIDENT SEVERITY SCHEMA

To facilitate appropriate escalation, GSOC will use a color-coded severity schema to categorize incident, breach, and event reports and define required escalation criteria and status update reporting expectations as long as the incident remains open. Incidents will be placed in the highest applicable tier of the schema based on currently available information. Bureaus should include their perceived severity as of the time of the report, but GSOC will officially assess the severity level. As additional information is available through investigation, the severity level of an incident may be altered.

GSOC will perform reporting to Treasury leadership using input provided by the Bureaus in the incident reporting system. While GSOC is responsible for providing updates to leadership for ongoing incidents, this requires cooperation from the appropriate Bureaus to provide updates to GSOC within established timeframes.

Table 3 - Treasury Cyber Incident Severity Schema

Severity	Criteria (any that apply)	Rationale	Examples	Minimum escalation level by GSOC[3]	Reporting expectations for bureaus to GSOC
Red (High)	1) "Major" or "significant cyber" incident 2) Functional impact = "Significant Impact to Critical Services" or "Denial of Critical Services / Loss of Control" 3) Information impact = "Critical Systems Data Breach" or "Core Credential Compromise" or "Destruction of Critical System" 4) Bureau/Dept issues press release or notifies Congress 5) PII loss ≥ 100,000 records	Likely to undermine confidence in Treasury, or to significantly impact Treasury's ability to perform its mission	PII loss > 100,000 records; Widespread destructive malware; HVA unavailable due to attack or failure; successful APT intrusion;	Secretary, Deputy Secretary, and Assistant Secretary for Management	Notification as quickly as possible after identification but no more than one business day. Status updates at least every 4 hours first day and at least daily thereafter.
Orange (Medium)	1) Functional impact = "Minimal Impact to Critical Services" or "Significant Impact to Non-Critical Services" 2) Recoverability = Not Recoverable 3) PII loss ≥ 100 records 4) Non-PII loss ≥ 100 records 5) Number of Users Affected ≥ 100	May undermine confidence in Treasury or somewhat impact Treasury's ability to perform its mission	Important system outage affecting usability; Website defacement; Significant malware infections or data loss;	Treasury CIO	Notification as quickly as possible after identification but no more than one business day Status updates at least daily.

[3] Further escalation at the discretion of the official receiving the report

Severity	Criteria (any that apply)	Rationale	Examples	Minimum escalation level by GSOC[3]	Reporting expectations for bureaus to GSOC
Yellow (Low)	1) Confirmed or suspected incident 2) Confirmed or suspected breach 3) Notable cyber event	Unlikely to impact Treasury's ability to perform its mission	Lost unencrypted device; single system malware infection; Blocked APT attack attempt; Paper PII loss of a single record	Treasury CISO	Notification as quickly as possible after identification but no more than one business day Status updates at least weekly.
White (Baseline)	1) Cyber event 2) Other tracked activities	Routine, unsubstantiated, or inconsequential event	Pen tests and exercises; Lost hardware with no risk	SOC	Optional but recommended. Status updates as required.

4.2.3.2 TREASURY INCIDENT STAKEHOLDER NOTIFICATION MATRIX

GSOC is the primary responsible party for ensuring appropriate Departmental and external resources are engaged during an incident. The following table describes the reporting and notification requirements for incidents, breaches, and events:

Table 4 - Cyber Incident Stakeholder Notification Matrix

LEGEND		RESPONSIBLE PARTY	TIMING
X	GSOC Incident Notification	GSOC	Varies by severity
I	GSOC Indicator Report	GSOC	Within 24 hours
Q	GSOC Quarterly Threat Report	GSOC	Quarterly
B	Bureau Report	Bureau	Next business day
L	Legislative Affairs Responsibility	Legislative Affairs	Within 7 days
P	PTR Responsibility	PTR	As Required

	EXTERNAL			INTERNAL															
CRITERIA (follow all that apply)	US-CERT	OMB	Congress	All Bureaus	Affected Bureau(s)	Treasury CISO	Treasury CIO	Asst. Sec. for Management	Deputy Secretary	Office of Critical Infrastructure Protection (OCIP)	Treasury Public Affairs	Treasury Leg Affairs	OIA/Counterintelligence	OIG (or TIGTA for IRS)	Privacy (PTR)	Security Programs (OSP)	Treasury Cyber Governance and Compliance	Treasury Operations Center (TOC)	Intelligence Operations Center (IOC)	Activate Enhanced Coordination Procedures (ECP)
Confirmed or suspected incident	x				x														
Major incident	x	x	L		x	x	x	x	x	x	x	x	x	x			x	x	x	x
APT - unsuccessful	I			I	Q	Q	Q						x	x						
APT - successful	x			I	x	x	x						x	x						
Cyber breach (PII involved)	x				x			P						x	x					
Non-cyber breach (PII involved)					x			P							x					
Red cyber incident					x	x	x	x	x	x				x				x	x	
Orange cyber incident	x				x	x	x							x						
Spill onto unclassified LAN	x				x								x			B				
Potential for media coverage					x	x	x	x	x	x	x		x	x				x	x	
Systemic risk/impact to the Department				x	x	x	x			x			x	x				x	x	
Potential insider threat	x				x								x							

4.2.3.3 MAJOR AND SIGNIFICANT INCIDENTS

GSOC is ultimately responsible for officially determining if an incident or breach constitutes a "major incident" and/or a "significant cyber incident." However, GSOC will consult with the affected bureau in order to make this determination. Furthermore, GSOC may consult with US-CERT on whether an incident is considered a "major incident" based on OMB's definition.

When GSOC declares a major incident has occurred, the following activities will take place:

- GSOC will update US-CERT when an incident has been declared a major incident. US-CERT will then notify OMB.
- GSOC will work with the Office of Legislative Affairs to ensure Congressional notification occurs within seven days of the date on which the Department has a reasonable basis to conclude that a major incident has occurred.
- After the initial notification to Congress of a major incident, the Department must provide to Congress additional information. GSOC will coordinate with the bureau and appropriate other stakeholders to gather this information and ensure the appropriate follow up reports are completed. The requirements are:
    - For a major incident, the Department must submit additional reports within a reasonable amount of time which include summaries of the threats, actors, risks, previous risk assessments of the affected system, the current status of the affected system, and the detection, response, and remediation actions that were taken.
    - For a major incident that is a breach, agencies must supplement the initial 7 day notification with a report no later than 30 days after the agency discovers the breach. The report must include a summary of information available about the breach, how the breach occurred, an estimate of the number of individuals affected by the breach, an assessment of the risk of harm to affected individuals, a description of any circumstances necessitating a delay in providing notice to affected individuals, and an estimate of whether and when the agency will provide notice to affected individuals.
- GSOC will activate the Emergency Coordination Procedures, as documented by the Department's Office of Critical Infrastructure Protection and required by PPD-41, if the major incident is also a significant cyber incident.

4.3 CONTAINMENT, ERADICATION, MITIGATION, AND RECOVERY

Incident response strategies will vary according to the nature of the incident as well as the different Bureau infrastructure and services provided. Response strategies outlined in this Departmental IRP are to be implemented where applicable and adjusted where needed. Response strategies formulated to address specific incidents will be informed by applicable bureau and system incident response and recovery plans.

Upon identification of an incident, the bureau, in collaboration with the GSOC, will evaluate risk associated with the current state of the affected system. Containment, mitigation, and recovery procedures will then be determined based upon calculated risk. Bureaus retain primary responsibility for formulating and executing response and recovery actions, but GSOC is available to assist bureaus with strategizing and performing such actions. GSOC may also issue directions regarding required bureau response actions.

Bureaus are required to inform GSOC about response and recovery action plans in response to incidents as they are formulated and provide updates as they are executed. Response and recovery plans in response to an incident should focus on first containing the incident and developing plans for interim operating capability for systems or business processes. This should then be followed by plans for fully mitigating the compromise, performing actions to prevent further or future compromise, and when applicable, recovering the system to return to full service.

Some of the measures that may be taken include but are not limited to:

- Blocking malicious indicators or traffic
- Capturing forensic evidence
- Collection and storage of all applicable logs for review
- Changing affected system passwords
- Disabling affected user accounts
- Shutting down affected systems
- Reimaging or replacing affected systems
- Restoring data or systems from backup
- Establishing out of band communications for incident response coordination
- Performing customer or stakeholder notifications about system impacts

In the event of a severity Orange or Red incident, GSOC will evaluate convening an IR team to discuss plans and updates regarding response and recovery efforts. The applicable Departmental stakeholders from the Stakeholder Notification Matrix will be included if such a team is convened. Furthermore, the bureau CSIRC will be expected to identify and include appropriate stakeholders as defined by their response and recovery plans.

Bureaus may wish to request additional resources to assist in incident response and recovery efforts. GSOC is available to provide technical support. Furthermore, Treasury has a standing Federal Network Authorization signed to request DHS on-site and/or technical assistance for IR. To activate that authorization, GSOC will email DHS after coordinating with the appropriate bureau(s). Bureaus may also procure surge support from incident response vendors.

4.3.1 SYSTEM SHUTDOWN

A bureau may elect to shutdown or isolate a bureau system if the system has been determined to pose an ongoing significant threat to Treasury systems, data, or customers and if the impact assessment and risk analysis suggests shutdown is the most prudent course of action when considering other operational needs of the Department. Furthermore, the GSOC, Treasury CIO, or Treasury Cybersecurity Board may direct a bureau to take such a response action. Bureaus must comply with such requests by initiating shutdown or isolation procedures on the affected system as expeditiously as possible. When shutting down or isolating the system, the bureau must ensure appropriate efforts are made to forensically capture the host image and active memory to aid in investigative efforts, if necessary or as directed by GSOC.

4.3.2 SYSTEM RECOVERY

In the event that an incident causes significant degradation or shutdown (voluntary or otherwise) of a system, bureaus must ensure coordination between incident responders and system recovery personnel. Bureaus must maintain recovery plans and procedures, whether in the form of information system contingency plans, disaster recovery plans, or incident recovery plans. At a minimum, such plans should identify the parties authorized to activate the plan and recovery team members, and should include pertinent information regarding service level agreements, recovery facilities, off-site storage, system-specific recovery details and procedures, details regarding access to the infrastructure, hardware, and software to provide intermediary services used during the recovery process, and operational work-arounds to apply during recovery periods.

Prior to restarting a system taken down as a result of an incident, the bureau must alert the GSOC. In accordance with PPD-41, prior to restarting a system where a significant cyber incident had an impact on multiple federal agencies or on the integrity, confidentiality, or availability of services to the public, the bureau must first coordinate with the GSOC, who will also coordinate with OMB and other applicable federal agencies to obtain a consolidated, timely written recommendation, with appropriate caveats and conditions, from those external parties to inform Treasury's decision to restart. Bureaus must also notify the GSOC at the completion of system recovery activities.

4.3.3 BREACHES

4.3.3.1 BREACHES AFFECTING TREASURY PERSONNEL OR CONTRACTORS

Bureaus must establish procedures to notify the appropriate Human Resource Officer (or his/her designee) or other bureau office, of breaches that involve the compromise or loss of PII associated with Treasury personnel or contractors. The procedures should address means for identifying the supervisors of persons involved in the incident and whether the circumstances of the incident suggest that corrective action is necessary.

4.3.3.2 BREACH NOTIFICATION

After evaluating the risk of harm, the bureau, in coordination with the breach response team when applicable, is responsible for advising the head of the agency on whether and whether to notify individuals potentially affected by a breach. Bureaus should draft their breach response plans in a manner consistent with relevant requirements in Treasury Directive 25-08, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.* This includes notifying the Departmental Personally Identifiable Information Risk Management Group (PIIRMG) (through the DASPTR) prior to issuing a breach notification in the event that the Bureau Head or designee determines that a breach has ramifications beyond the affected bureau or cannot be adequately addressed by the affected bureau alone.

If after conducting the appropriate risk analysis, the bureau determines that victim notification is warranted, the bureau should notify affected individuals, in accordance with FISMA 2014, as "expeditiously as practicable, without unreasonable delay." Bureaus must notify those individuals within 30 days unless directed otherwise by an appropriate law enforcement entity, including Treasury's Inspectors General and the Special Inspector General for the Troubled Asset Relief Program, because notification would interfere with an ongoing law enforcement matter. Bureaus must also track and report to GSOC how long it took to send victim notifications and what percentage of notifications was sent within 30 days. Bureaus should coordinate these victim notification activities with the Treasury Office of Public Affairs, as well as their own public affairs offices. If a determination is made to notify individuals potentially affected by the breach, Bureaus must follow OMB guidance for:

(1) Identifying the source of the Notification (e.g., Treasury, bureau or contractor);

(2) Timeliness of the notification (as expeditiously as practicable, without unreasonable delay);

(3) The contents of the notification (e.g., whether to draft different notifications for different potentially affected populations);

(4) Method of notification (depending on the circumstances of a breach); and,

(5) Special considerations (e.g., tailoring the notification for vulnerable populations, and individuals who are visually or hearing impaired).

Bureaus can provide notification to victims in any manner they deem adequate but it will always include First-Class mail notification to the last known mailing address of the individual in Treasury records. The notification letter will include the bureau logo.

4.3.3.3 BREACH REMEDIATION

Bureaus should also consider providing identity monitoring services to individuals who are impacted by a breach that has a substantial likelihood of causing harm. Bureaus other than the Internal Revenue Service should contact the Departmental Cyber Security Office and Office of Public Affairs for a Standard Operating Procedure for General Services Administration Blanket Purchase Agreements.

In the event that victim notification could compromise ongoing investigations or involve law enforcement, notification may be delayed if disclosure of the investigation pertaining to the breach of PII or to an individual impacted by the breach of PII would seriously impede the investigation of the impacted individual. However, any delay should not exacerbate risk or harm to any impacted individual(s).

4.4 POST-INCIDENT ACTIVITY

4.4.1 POST-INCIDENT ANALYSIS

After any incident of Orange or Red severity, the bureau or GSOC, as appropriate, must complete an after action or analysis report. In the event of a lower-level event, such a report should be produced only if it would be of value to the bureau or the Department. Potential questions to consider in such a report include:

- Exactly what happened, and at what times?
- What is the overall damage or impact from the incident?
- How well did staff and management perform in dealing with the incident?
- Were the documented response and recovery plans followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

As appropriate, the GSOC will facilitate sharing lessons learned throughout the Department so all bureaus can learn from each incident.

4.4.2 REPORTING AND METRICS

The bureaus will maintain detailed summaries of incidents and breaches and their subsequent investigations within the incident reporting system. Treasury must be able to track and monitor the following:

- The total number of incidents and breaches reported over a given period of time;
- The status for each reported incident, including whether the bureau's response to that incident is ongoing or has concluded;
- The time elapsed:
    - From incident occurrence to detection
    - From detection to initial investigation
    - From initial investigation until report to GSOC
    - From GSOC report receipt to US-CERT report (where applicable)
    - From initial investigation until resolution
- For at least all Orange and Red incidents, a damage assessment, to include:
    - Service outage or system downtime periods
    - Costs incurred, including hardware, software, labor, service, or any other applicable costs
- In the event of a breach:
    - The number of individuals potentially affected by each reported breach;
    - The types of personally identifiable information potentially compromised by each reported breach;
    - Whether the bureau, after assessing the risk of harm, provided notification to the individuals potentially affected by a breach;
    - If notifications were sent, the elapsed time between breach confirmation and notification issuance;

At the end of each quarter, GSOC will facilitate sharing of reports/metrics and lessons learned throughout the Department so all bureaus can learn from each incident and breach. This will be used a benchmark to ascertain bureaus' progress in implementing effective practices from lessons learned. As appropriate, the GSOC will facilitate sharing lessons learned throughout the Department so all bureaus can learn from each incident. This will assist the Department in compliance reviews, remediation of audit findings, and reporting requirements.

5. ACRONYMS

APT Advanced persistent threat

CAP Cybersecurity Administration Priorities

CIO Chief Information Officer

CIOC Treasury CIO Council

CIP Critical Infrastructure Protection

CISO Chief Information Security Officer

CSIRC Computer Security Incident Response Center

DASPTR Deputy Assistant Secretary for Privacy, Transparency, and Records

DHS Department of Homeland Security

GSOC Government Security Operations Center

HVA High value asset

IOC Indicator of Compromise

IR Incident response

IRP Incident response plan

NCCIC National Communications, Coordination, and Integration Center

OCI Office of Counterintelligence

OCIO Office of the Chief Information Officer

OCIP Office of Critical Infrastructure Protection and Compliance Policy

OIG Office of the Inspector General

OMB Office of Management and Budget

OSP Office of Security Programs

PII Personally Identifiable Information

PIIRMG PII Response Management Group

PPD Presidential Policy Directive

PTR Office of Privacy, Transparency, and Records

SAOP Senior Agency Official for Privacy

TCSIRC Treasury Computer Security Incident Response Center

TD Treasury Directive

TD P Treasury Directive Publication

TFIMS Treasury FISMA Inventory Management System

TIC Trusted Internet Connection

TIGTA Treasury Inspector General for Tax Administration

TCB Treasury Cybersecurity Board

TS/SCI Top Secret/Specialized Compartmented Information

US-CERT United States Computer Emergency Readiness Team

APPENDIX

Appendix A - Impact Classification Descriptions by US-CERT

Impact Category	Category Severity Levels
Functional Impact – A measure of the impact to business functionality or ability to provide services	NO IMPACT – Event has no impact.
	NO IMPACT TO SERVICES – Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers.
	MINIMAL IMPACT TO NON-CRITICAL SERVICES – Some small level of impact to non-critical systems and services.
	MINIMAL IMPACT TO CRITICAL SERVICES –Minimal impact but to a critical system or service, such as email or active directory.
	SIGNIFICANT IMPACT TO NON-CRITICAL SERVICES – A non-critical service or system has a significant impact.
	DENIAL OF NON-CRITICAL SERVICES – A non-critical system is denied or destroyed.
	SIGNIFICANT IMPACT TO CRITICAL SERVICES – A critical system has a significant impact, such as local administrative account compromise.
	DENIAL OF CRITICAL SERVICES/LOSS OF CONTROL – A critical system has been rendered unavailable.
Information Impact – Describes the type of information lost, compromised, or corrupted.	NO IMPACT – No known data impact.
	SUSPECTED BUT NOT IDENTIFIED – A data loss or impact to availability is suspected, but no direct confirmation exists.
	PRIVACY DATA BREACH – The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised.
	PROPRIETARY INFORMATION BREACH – The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
	DESTRUCTION OF NON-CRITICAL SYSTEMS – Destructive techniques, such as master boot record (MBR) overwrite; have been used against a non-critical system.
	CRITICAL SYSTEMS DATA BREACH - Data pertaining to a critical system has been exfiltrated.
	CORE CREDENTIAL COMPROMISE – Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated.
	DESTRUCTION OF CRITICAL SYSTEM – Destructive techniques, such as MBR overwrite; have been used against a critical system.

Impact Category	Category Severity Levels
Recoverability – Identifies the scope of resources needed to recover from the incident	REGULAR – Time to recovery is predictable with existing resources.
	SUPPLEMENTED – Time to recovery is predictable with additional resources.
	EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed.
	NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).

For the purposes of interpreting the Category Severity Levels, GSOC offers the following additional guidance:

- Critical systems are interpreted to mean any system designated as an HVA or CIP system
    - For GSS that are also designated HVA or CIP, this should interpreted to mean a device or service critical to the functioning of the GSS rather than any single device in the GSS. For example, a ransomware event infecting a single desktop would most likely not be "Destruction of a Critical System", but ransomware affective file shares with critical information would.
- Critical services are interpreted to mean a system or process essential to the functioning of the Department, either directly or in a supporting role. This includes functions designated as Mission Essential Functions, but is not necessarily limited to those functions. For example, in most cases, functioning of email would be considered a critical service even if the bureau GSS is not designated as an HVA.
- For unconfirmed information impact, bureaus should select "Suspected but not identified" in addition to the type of information impact for the incident, if known. For example, for a suspected PII loss, both "Suspected but not identified" and "Privacy Data Breach" should be selected.
- For these purposes, a destructive information impact could include:
    - Data alteration, such as unauthorized overwriting of records/data
    - Unauthorized encryption, such as ransomware, that at least temporarily precludes access to data
    - Data deletion
    - System destruction

Appendix B – Observed Activity Definitions

Activity	Definition
None	
Preparation	Activities undertaken by a threat actor, their leadership and/or sponsor to prepare for conducting malicious cyber activities, e.g., establish governance and articulating intent, objectives, and strategy; identify potential victims and attack vectors; securing resources and develop capabilities; assess intended victim's cyber environment; and define measures for evaluating the success or failure of threat activities.
Engagement	Threat actor activities taken prior to gaining but with the intent to gain unauthorized access to the intended victim's physical or virtual computer or information system(s), network(s), and/or data stores.
Presence	Actions taken by the threat actor once unauthorized access to victim(s)' physical or virtual computer or information system has been achieved that establishes and maintains conditions or allows the threat actor to perform intended actions or operate at will against the host physical or virtual computer or information system, network and/or data stores.
Effect/Consequence	Outcomes of threat actor actions on a victim's physical or virtual computer or information system(s), network(s), and/or data stores.

Appendix C – Incident Attributes Defined by US-CERT

Attribute Category	Attribute Definitions
Location of Observed Activity: Where the observed activity was detected in the network.	LEVEL 1 – BUSINESS DEMILITERIZED ZONE – Activity was observed in the business network's demilitarized zone (DMZ)
	LEVEL 2 – BUSINESS NETWORK – Activity was observed in the business or corporate network of the victim. These systems would be corporate user workstations, application servers, and other non-core management systems.
	LEVEL 3 – BUSINESS NETWORK MANAGEMENT – Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores.
	LEVEL 4 – CRITICAL SYSTEM DMZ – Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay "jump" boxes into more critical systems.
	LEVEL 5 – CRITICAL SYSTEM MANAGEMENT – Activity was observed in high-level critical systems management such as human-machine interfaces (HMIs) in industrial control systems.
	LEVEL 6 – CRITICAL SYSTEMS – Activity was observed in the critical systems that operate critical processes, such as programmable logic controllers in industrial control system environments.
	LEVEL 7 – SAFETY SYSTEMS – Activity was observed in critical safety systems that ensure the safe operation of an environment. One example of a critical safety system is a fire suppression system.
	UNKNOWN – Activity was observed, but the network segment could not be identified.
Actor Characterization	The type of actor(s) involved in the incident (if known). This element is not selected by the reporting entity.
Cross-Sector Dependency	A weighting factor that is determined based on cross-sector analyses conducted by the DHS Office of Critical Infrastructure Analysis (OCIA). This element is not selected by the reporting entity.
Potential Impact	An estimate of the overall national impact resulting from a total loss of service from the affected entity. This element is not selected by the reporting entity.

Note: Agencies are not required or expected to provide Actor Characterization, Cross-Sector Dependency, or Potential Impact information. These are assessed independently by NCCIC/US-CERT incident handlers and analysts. Additionally, Observed Activity is not currently required and is based on the attack vector, if known, and maps to the ODNI Cyber Threat Framework.

For the purposes of interpreting the incident attributes, GSOC offers the following additional guidance:

- For location of observed activity:
  - Use the highest level that applies in the event that more than one are applicable
  - Cloud/outsourced systems should be evaluated like they are an internal system
- Critical systems are interpreted to mean any system designated as an HVA or CIP system
  - For GSS that are also designated HVA or CIP, this should interpreted to mean a device or service critical to the functioning of the GSS rather than any single device in the GSS.

Appendix D – Example Incident Reporting Interpretations

Scenario # 1: Lost encrypted GFE mobile device (e.g., lost BlackBerry)

An end user reports loss of a GFE mobile device. Bureau configurations ensure device is password protected and that either the entire device is appropriately encrypted or all data resides in an encrypted container. There are no extenuating circumstances that indicate the device may have been inappropriately accessed or at increased risk of being inappropriately accessed.

GSOC Report Required: No

US-CERT Report Required: No

Correct incident report selections:
Functional Impact: No Impact
Information Impact: No Impact
Recoverability: Regular
Threat Vector: Loss or Theft of Equipment
Location of Observed Activity: Level 2 – Business Network
Incident Severity: White

NOTE: Even though GSOC reporting is not required, bureaus should still perform remediation actions, such as remotely wiping the lost device. Furthermore, bureaus should likely also track such actions on their own for metrics and asset inventory purposes. Finally, in the case where a bureau has reason to believe the device may have been at risk for compromise (e.g., bureau learns the user taped the unlock password to the device itself), this would then become a reportable incident.

Scenario # 2: Single Record Paper PII Loss

A Treasury user mails a single PII record to the wrong recipient.

GSOC Report Required: Yes

US-CERT Report Required: Yes

Correct incident report selections:
Functional Impact: No Impact
Information Impact: Privacy Data Breach
Recoverability: Not Recoverable
Threat Vector: Improper Usage
Location of Observed Activity: Level 2 – Business Network
Incident Severity: Yellow

Scenario # 3: Desktop AV quarantined malware – unsuccessful

A Treasury desktop antivirus detects malware installation attempt and quarantines malware prior to infection.

GSOC Report Required: No

US-CERT Report Required: No

Correct incident report selections:
Functional Impact: No Impact
Information Impact: No Impact

Recoverability: Not Applicable
Threat Vector: [Varies]
Location of Observed Activity: Level 2 – Business Network
Incident Severity: White

Scenario # 4: Desktop infected with malware

A Treasury desktop is infected with routine malware. In this case, the malware did not appear to steal or destroy data.

GSOC Report Required: Yes

US-CERT Report Required: Yes

Correct incident report selections:
Functional Impact: No Impact to Services
Information Impact: No Impact
Recoverability: Regular
Threat Vector: [Varies]
Location of Observed Activity: Level 2 – Business Network
Incident Severity: Yellow

Scenario # 5: Use of stolen credentials to inappropriately access data in a public facing system

A Treasury public-facing system is inappropriately accessed by an outsider who was successfully able to impersonate an end user using compromised PII. At this point, it is unknown if the attacker was able to gain access to steal additional PII, but the potential loss is expected to affect >100 users. The accessed system is deemed to be a High Value Asset.

GSOC Report Required: Yes

US-CERT Report Required: Yes

Correct incident report selections:
Functional Impact: No Impact
Information Impact: Suspected but not identified & Privacy Data Breach
Recoverability: [Varies]
Threat Vector: Impersonation/Spoofing
Location of Observed Activity: Level 1 – Business Demilitarized Zone
Incident Severity: Orange

Scenario #6: Targeted spear phishing email with no compromise

A targeted spear phishing email was identified. The email was mitigated without the user clicking the link or opening the attachment, therefore no machine compromise occurred.

GSOC Report Required: Yes

US-CERT Report Required: No

Correct incident report selections:
Functional Impact: No Impact
Information Impact: No Impact
Recoverability: Not applicable
Threat Vector: Email/Phishing
Location of Observed Activity: Level 2 – Business Network

Incident Severity: Yellow

Scenario #7: Unexplained potential beaconing

A Treasury system is initiating suspicious outbound traffic, but the exact cause is unknown. After a reasonable effort, no legitimate explanation for this traffic can be found.

GSOC Report Required: Yes

US-CERT Report Required: Yes, if GSOC investigation cannot rule out.

Correct incident report selections:
Functional Impact: No Impact
Information Impact: No Impact
Recoverability: Not applicable
Threat Vector: Unknown
Location of Observed Activity: Level 2 – Business Network
Incident Severity: Yellow

Scenario #8: Lost item that doesn't contain data

A loss of any of the following items: RSA token, PIV card, computer monitor, or other similar devices.

GSOC Report Required: No

US-CERT Report Required: No

Correct incident report selections:
Functional Impact: No Impact
Information Impact: No Impact
Recoverability: Regular
Threat Vector: Loss or Theft of Equipment
Location of Observed Activity: Level 2 – Business Network
Incident Severity: White

NOTE: Even though GSOC reporting is not required, bureaus should still perform remediation actions, such as disabling access for a lost token. Furthermore, bureaus should likely also track such actions on their own for metrics and asset inventory purposes. Finally, in the case where a bureau has reason to believe the loss may have subsequently led to a compromise or increased risk of compromise (e.g., the lost RSA token was used to access a system), this would then become a reportable incident.

Scenario #9: Ransomware infection that encrypts critical file repositories

A Treasury GSS is infected with ransomware that successfully encrypted important file repositories but doesn't degrade Treasury's ability to perform its mission in the short term.

GSOC Report Required: Yes

US-CERT Report Required: Yes

Correct incident report selections:
Functional Impact: Minimal Impact to Critical Services
Information Impact: Destruction of Non-Critical System
Recoverability: [Varies]
Threat Vector: [Varies]

Location of Observed Activity: Level 2 – Business Network
Incident Severity: Orange

Scenario #10: Compromise of domain admin credentials by an external attacker

An external intruder was able to infiltrate the Treasury network and successfully obtain domain administrator access

GSOC Report Required: Yes

US-CERT Report Required: Yes

Correct incident report selections:
Functional Impact: Significant Impact to Critical Services
Information Impact: Core Credential Compromise
Recoverability: Extended
Threat Vector: [Varies]
Location of Observed Activity: Level 3 – Business Network Management
Incident Severity: Red

Scenario #11: Malicious insider steals sensitive PII and business data, over 10,000 records, using thumb drive

A user using an unauthorized thumb drive was able to steal sensitive data, including over 10,000 but less than 100,000 records of PII and business data.

GSOC Report Required: Yes

US-CERT Report Required: Yes

Correct incident report selections:
Functional Impact: No Impact
Information Impact: Privacy Data Breach, Proprietary Information Breach
Recoverability: Regular or Not Recoverable
Threat Vector: Removable Media
Location of Observed Activity: Level 2 – Business Network
Incident Severity: Red

Scenario #12: Remote compromise of a public-facing HVA system where attacker gained administrative access and system had to be disabled

Incident of a critical application where the system had to be disabled after the attacker gained administrative access. Information impact currently unknown, but system contains PII.

GSOC Report Required: Yes

US-CERT Report Required: Yes

Correct incident report selections:
Functional Impact: Denial of Critical Service
Information Impact: Suspected but not identified and Privacy Data Breach
Recoverability: Extended
Threat Vector: [Varies]
Location of Observed Activity: Level 6 – Critical Systems
Incident Severity: Red

Appendix E – FAQs for Major Incidents

Who will send the Congressional notification?

The Department's Legislative Affairs office will be responsible for executing the Congressional notification unless the bureau Legislative Affairs office coordinates an alternative execution plan with the bureau. In such cases, the Department is to be so advised and must be provided with a copy of the Congressional notification.

What external parties need to be notified?

U.S. House of Representatives:

- Chairman, Committee on Oversight and Government Reform
- Ranking Member, Committee on Oversight and Government Reform
- Chairman, Committee on Homeland Security
- Ranking Member, Committee on Homeland Security
- Chairman, Committee on Science, Space and Technology
- Ranking Member, Committee on Science, Space and Technology
- Chairman and Ranking member of the appropriate authorization and appropriations committees, such as:
    - Committee on Ways and Means
    - Committee on Appropriations

United States Senate

- Chairman, Committee on Homeland Security and Governmental Affairs
- Ranking Member, Committee on Homeland Security and Governmental Affairs
- Chairman, Committee on Commerce, Science and Transportation
- Ranking Member, Committee on Commerce, Science and Transportation
- Chairman and Ranking member of the appropriate authorization and appropriations committees, such as:
    - Committee on Finance
    - Committee on Appropriations

Notifications are not required to the OMB Director, DHS Secretary, and Comptroller General. These individuals receive the annual FISMA report only.

How should the notification occur?

Per OMB guidance, the initial notification can occur in writing, such as a memo, or via phone. However, Treasury should issue written notification if at all possible to ensure we have a clear record of what was said and when.

When is the initial notification due and what should it say?

Congressional notification is required within seven days of the date on which the Department has a reasonable basis to conclude that a major incident has occurred. This is measured from the time GSOC officially declares and notifies US-CERT that an incident has been deemed a major incident.

There are no specific guidelines on required data elements for the initial notification in external guidance. Minimally, the notification should include brief introduction as to why this notification is being submitted, and a brief explanation of the incident in question as appropriate and using information known at that time, including an explanation of the affected system, and any high level detection, analysis, response, and remediation actions taken or planned to date.

What follow up reports are required and when?

For a major incident, the Department must submit additional reports to the Congressional stakeholders within a reasonable amount of time which include summaries of the threats, actors, risks, previous risk assessments of the affected system, the current status of the affected system, and the detection, response, and remediation actions that were taken.

For a major incident that is a breach, agencies must supplement the initial 7 day notification with a report no later than 30 days after the agency discovers the breach. The report must include a summary of information available about the breach, how the breach occurred, an estimate of the number of individuals affected by the breach, an assessment of the risk of harm to affected individuals, a description of any circumstances necessitating a delay in providing notice to affected individuals, and an estimate of whether and when the agency will provide notice to affected individuals.

This supplemental information will also be included in the annual FISMA report.

Who can I ask for help with notifications?

Reach out to the GSOC if you need assistance, and GSOC will find the appropriate resource.

Do you have any example notifications?

Below is an anonymized example based on a real notification.

January 1, 2017

The Honorable Jason Chaffetz
Chairman, Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Chaffetz:

In accordance with the requirements of the Federal Information Security Modernization Act (FISMA) and criteria provided in guidance from the Office of Management and Budget (OMB), this letter provides notice that the ***AGENCY NAME*** has identified a major incident involving the ***APPLICATION NAME***. FISMA requires agencies to report major incidents to the Congress "not later than seven days after the date on which there is reasonable basis to conclude that a major incident has occurred."

The ***APPLICATION NAME*** is ***DESCRIPTION OF APPLICATION FUNCTION***. On ***January 1, 2017***, we became concerned about ***the misuse of the application*** by criminals masquerading as ***AGENCY CONSTITUENTS or CUSTOMERS***. Protecting ***sensitive agency*** information is our highest priority. We therefore disabled the ***APPLICATION NAME*** on ***January 3***, and it will remain unavailable until ***commensurate safeguards*** can be added.

We began determining the affected community immediately and began notifying impacted ***CONSTITUENTS or CUSTOMERS*** on ***January 7, 2017***. In accordance with FISMA guidance, additional details will be forthcoming including summaries of our detection, response, and remediation activities.

We are working closely with ***AFFECTED STAKEHOLDERS and/or PARTNER AGENCIES*** to safely return the ***APPLICATION NAME*** to service as soon as possible. If you have additional questions, please call me, or a member of your staff may call ***ALTERNATE POC***, ***TITLE***, ***DEPARTMENT or BUSINESS UNIT***, at ***202-ddd-dddd***.

Sincerely,

AGENCY HEAD NAME