DEPARTMENT OF HOMELAND SECURITY Cybersecurity and Infrastructure Security Agency

OMB Control No: 1670-0037

Expiration Date: 12/31/2021

INCIDENT REPORTING FORM

<u>PURPOSE:</u> The Incident Reporting Form enables U.S. Federal Government agencies and external entities to report security incidents, major incidents, breaches, and events under investigation to the Cybersecurity and Infrastructure Security Agency (CISA). The information is used by CISA to provide appropriate responses to affected entities and to gain greater insights into security threats.

NOTE: Do <u>not</u> add sensitive personally identifiable information (SPII) to incident submissions. Any contact information collected will be handled according to the <u>Department of Homeland Security (DHS) privacy policies.</u>

Paperwork Reduction Act

The public reporting burden to complete this information collection is estimated at 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the collected information. The collection of information is required to obtain a benefit. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to DHS/CISA, 245 Murray Lane, SW, Mail Stop 0640, Arlington, VA 20598-0640 ATTN: PRA [OMB Control No. 1670-0037].

			REPORTING	3 BASI	ics		
View the updated FIRR	requireme	nts for descripti	ons of the differen	t reporti	ing categories.		
1. Are you reporting an i	ncident, m	ajor incident, bi	each, or Event un	der Inve	estigation at thi	s time?	
☐ Incident ☐ Major	Incident	Breach	Event Under In	nvestiga	ation		
2. What type of report ar	e you subi	mitting?					
One-Hour Initial Rep	ort 🔲 7	72-Hour Initial F	Report 72-Ho	our Upd	late Post	Incident/Major Incid	dent Breach Update
		INCIDE	ENT REPORTIN	G REC	QUIREMENTS	3	
		ONE	-HOUR INITIAL II	NCIDE	NT REPORT		
The below elements are	required (if available) who	en reporting an inc	cident to	CISA for the f	irst time:	
1. User Type: Impac	cted User	Reporting	on Behalf of the I	mpacte	d User		
2. Name of Reporter							
A. First: B. Middle (if applicable):			pplicable):	C.	Last:	D. Suffix (if applicable):	
						ation (i.e., soc@orga	anization.gov,
A. Unclassified:	B. Classi	fied:	soc@organization.com):				
5. Top-Level Organization	on						
A. Name: B. Type:							
C. Point(s) of Contact							
1. Name							
First: Middle (if appl		icable): Last:		st:		Suffix (if applicable):	
2. Phone Number(s)			3. Email Address				
Unclassified:	Classifie	d:	Unclassified: Classified:				
6. Organization Sub-Ent	ity:			7. C	ritical Infrastruc	ture Sector:	
8. Identify the current level of impact on agency functions or services (Functional Impact):							

CISA Form X (8/19) Page 1 of 42

INCIDENT REPORTING REQUIREMENTS						
ONE-HOUR INITIAL INCIDENT REPORT (CONTINUED)						
9. Estimate the scope of time and resources needed to recover from the incident (Recoverability):						
10. On-site or remote assistance required?						
Yes No If yes, identify:						
11. Are the impacted system(s) Federal Information Security Modernization Act of 2014 (FISMA)¹ system(s)?²						
Yes No If yes, provide name of system(s):						
12. Is this a High Value Asset? 13. When was the activity first detected?						
☐ Yes ☐ No						
14. What detection methods were used to discover this activity?						
Administrator Intrusion Detection System (IDS) User Other Anti-Virus Software Log Review Unknown						
15. What date and time was the incident declared? (Universal Time Coordinated [UTC] or local time with UTC offset)						
Date: Time:						
16. How many of the following were impacted?						
☐ Systems						
Endpoints						
☐ Operating Systems☐ Server Types						
Email						
Network Devices						
Routers Firewalls IDS Load Balancers Other Switches Proxies Intrusion Protection System (IPS) Hub						
☐ Users						

CISA Form X (8/19) Page 2 of 42

^{1 44} U.S.C. §§ 3551-3558.

Pursuant to FISMA, an "information system" is defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

INCIDENT REPORTING REQUIREMENTS							
ONE-HOUR INITIAL INCIDENT REPORT (CONTINUED)							
17. What network location(s) and information system(s) was the activity observed in?							
17A. What network segment(s) or	r Virtual Local <i>I</i>	Area Network(s) was th	ne activity observed	in?			
18. Describe the nature of the activity:							
19. Describe how the events were							
20. Have any actions been taken		Are you also reporting					
recover from the incident? Yes No	I — .	unauthorized access to Yes	, refer to the breach		•		
22. Identify the points of contact a point of contact is preferred).	and contact det	ails for additional follo	w-up (a 24-hours pe	r day, 7 days per w	veek operations center		
A. Name							
First:	Middle (if ap	plicable):	Last:		Suffix (if applicable):		
B. Phone Number(s)		C. Ema	ail Address			
Unclassified: Classified	ed:	Unclassified:		Classified:			
23. Did this incident involve an unattributed cyber intrusion?							
Yes No If yes, answ							
A. Understanding the Victim	A. Understanding the Victim						
1. Defense and Weapons Systems Observed network intrusion or penetration? Yes No Observed access to data storage or file systems? Yes No Observed access to control systems? Yes No							
2. Financial Sector Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Yes No No							
 Government and Support Net Observed network intrusion or Observed access to data stora Observed access to control sy 	penetration? age or file syste	ems? Yes	No No No				
4. Health and Public Safety Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Yes No Yes No							
5. National Communications and Technology Infrastructure Observed network intrusion or penetration?							

CISA Form X (8/19) Page 3 of 42

 $[\]overline{^3}$ Providing these metrics enables CISA to prioritize unattributed cyber intrusions for further analysis.

INCIDENT REPORTING REQUIREMENTS						
ONE-HOUR INITIAL INCIDENT REPORT (CONTINUED)						
A. Understanding the Victim (Continued)						
6. Public Transportation Observed network intrusion or penetration?						
7. Public Utilities Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Yes No Yes No						
B. Recognizing Impact and Effects						
1. Observed impact to domestic or foreign policy? 2. Observed impact to government operations? 3. Observed impact to national or global financial systems or economy? 4. Observed impact to intellectual property? 5. Observed impact to domestic or foreign reputation of governments or corporations? Yes No						
C. Identifying Techniques and Motivations						
1. Sophistication Human-enabled or close-access operations? Complex delivery or exfiltration techniques? Custom, tailored, or unique tool(s) used? Complex obfuscation techniques? Established persistence? Yes No Yes No Yes No Yes No Yes No Strategic Direction						
Targeted intrusions against strategic targets? Specificity of data or information stolen or manipulated? Aligned with global or political event? Aligned with known foreign government policies? Yes No No No						
D. Estimating Publicity						
1. Is the government tracking this or similar incidents? 2. Is there national media coverage or other widely available public coverage? 3. Are foreign state adversaries tracking this incident? 4. Are foreign non-state adversaries tracking this incident? 5. Are discussions about the incident taking place in online communities? Yes No No No						
24. Using the matrices from the MITRE ATT&CK™⁴ framework, list all adversarial tactics and techniques that relate to this incident below:						
A. If the incident involved Windows, Mac, or Linux platforms, utilize the Enterprise Matrix ⁵ :						

CISA Form X (8/19) Page 4 of 42

⁴© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation and in accordance with the Terms of Use available here: https://attack.mitre.org/resources/terms-of-use/. CISA, DHS, or the U.S. Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA, DHS, or the U.S. Government.

⁵ Information on tactics and techniques from the Enterprise Matrix can be found at https://attack.mitre.org/matrices/enterprise.

INCIDENT REPORTING REQUIREMENTS					
ONE-HOUR INITIAL INCIDE	NT REPORT (CONTINUED)				
B. If the incident involved access to a mobile device, utilize the Mo	bile Device Access Matrix ⁶ :				
C. If the incident involved network-based effects, not necessarily li Effects Matrix ⁷ :					
72-HOUR INCIDENT UPDATE (CONTINUOUS UN	ITIL ALL ERADICATION ACTIVITES COMPLETE)				
The below elements are <u>required</u> (if available) when reporting to C	ISA:				
On-site or remote assistance required?					
Yes No If yes, identify:					
2. Are you upgrading this incident to a major incident?	No				
2A. If yes, please provide justification:					
Are you also reporting a breach at this time (i.e., confirmed or poinformation records)? Yes No If yes, refer to the breach reporting requirements.					
Substantive updates <u>required</u> , provide if available:					
A. Attack Vector(s):					
That led to the incident:	Detected during the course of investigation:				
B. Indicators of Compromise (IOC):	Toutto Links Doube and Only				
IOC:	Traffic Light Protocol Color:				
Indicator Title:	Indicator Description:				
IOC Kill-Chain Step:	Countermeasure(s):				
Should the cyber threat indicator or defensive measure contained in this submission be considered commercial, financial, and proprietary information submitted by a non-federal entity, as defined, to the U.S. Federal Government under the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. § 1504(d)(2))?					
4C. Domains Associated with the Incident:					

CISA Form X (8/19) Page 5 of 42

⁶ Information on tactics and techniques from the Mobile Device Access Matrix can be found at https://attack.mitre.org/matrices/mobile.

⁷ Information on tactics and techniques from the Mobile Network-Based Effects Matrix can be found at https://attack.mitre.org/matrices/mobile.

INCIDENT REPORTING REQUIREMENTS					
72-HOUR INCIDENT UPDATE (CONTINUOUS UN	TIL ALL ERADICATION ACTIVITES COMPLETE) (CONTINUED)				
4D. Internet protocol (IP) addresses and their relation to the	e incident (such as attacker and victim):				
4E. Malicious software or malicious scripts detected (by hu States Computer Emergency Readiness Team website	mans or Personal Security Products) via "Report Malware" on the United :				
4F. Mitigation activities undertaken in response to the incid	ent:				
4G. Description of how the incident occurred:					
4H. How the incident was identified:					
4I. How many of the following were impacted?					
Systems					
Endpoints					
Operating SystemsServer Types					
Email File Print Web Cloud Kerberos TELNET Secure Shell (SSH) Remote Shell (RSH) Certificate Authority (CA) Virtual Private Network (VPN) Domain Name System (DNS) File Transfer Protocol (FTP)	Network Time Protocol (NTP) Active Directory (AD) Components Voice over Internet Protocol (VoIP) Gateways Security Information and Event Management (SIEM) Dynamic Host Configuration Protocol (DHCP) Remote Log(s) (i.e., Email, VPN, Syslog, R-Syslog, Syslog-NG) Authentication, Authorization, and Accounting (AAA) Services (i.e., Radius, Terminal Access Controller Access-Control System [TACACS+]) Lightweight Directory Access Protocol/Lightweight Directory Access Protocol over Secure Sockets Layer (LDAP/LDAP[S]) Other				
Network Devices					
Routers Firewalls IDS Switches Proxies Intrusion	Load Balancers Other Protection System (IPS) Hub				
Users					

CISA Form X (8/19) Page 6 of 42

INCIDENT REPORTING REQUIREMENTS
72-HOUR INCIDENT UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITES COMPLETE) (CONTINUED)
4J. Based on the phase of the incident response process ⁸ , provide the following:
a. Strategy:
a. Stategy.
b. As an update, was the containment strategy successful:
c. If unsuccessful, provide details on how your strategy is changing:
2. Eradication
a. Strategy:
b. As an update, was the eradication strategy successful:
c. If unsuccessful, provide details on how your strategy is changing:
4K. Provide upon request and if available (with the documentation or agreement to provisions as requested by CISA):
Memory captures from information systems where threat actor activity was identified or suspected:
2. System logs from compromised systems (starting from 24-hours prior to the first event identified in the incident, through the present time):
Application:
System Security:
Other logs collected by the system(s) and/or application(s):
3. Network logs (starting from 24-hours prior to the first event identified in the incident, through the present time) detailing communication from the impacted host(s). Logs include, but are not limited to: DHCP, DNS, Firewall, Packet Capture, Host, Hypervisor, Netflow, Network Device, Proxy, and HyperText Transfer Protocol/HyperText Transfer Protocol Secure:
4. Provide a timeline of identified or suspected compromised systems communicating with other systems. Network artifacts include, but are not limited to: Source IP Address, Source Hostname, Source Fully Qualified Domain Name (FQDN), Source Port, Destination IP Address, Destination Hostname, Destination FQDN, Destination Port, Transport Protocol, Application Protocol, Communication Start Time (UTC or local time with UTC offset), and Communication End Time (UTC or local time with UTC offset).

CISA Form X (8/19) Page 7 of 42

⁸ National Institute of Standards and Technology Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide. U.S. Department of Commerce. August 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

T2-HOUR INCIDENT UPDATE (CONTINUOUS UNTIL ALL E Did this incident involve an unattributed cyber intrusion? Yes No If yes, answer whether each of the following even	
Yes No If yes, answer whether each of the following ever	nts was observed. ⁹
	nts was observed.9
A. Understanding the Victim	
1. Defense and Weapons Systems Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Yes Yes	☐ No ☐ No ☐ No
2. Financial Sector Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Yes Yes	□ No□ No□ No
3. Government and Support Networks Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Yes	☐ No ☐ No ☐ No
4. Health and Public Safety Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Yes Yes	NoNoNoNo
5. National Communications and Technology Infrastructure Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Yes Yes	NoNoNoNo
6. Public Transportation Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Yes Yes	☐ No ☐ No ☐ No
7. Public Utilities Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Yes Yes	NoNoNoNo
B. Recognizing Impact and Effects	
 Observed impact to domestic or foreign policy? Observed impact to government operations? Observed impact to national or global financial systems or economy Observed impact to intellectual property? Observed impact to domestic or foreign reputation of governments 	Yes No
C. Identifying Techniques and Motivations	
1. Sophistication Human-enabled or close-access operations? Complex delivery or exfiltration techniques? Custom, tailored, or unique tool(s) used? Complex obfuscation techniques? Established persistence? Yes	 No No No No No No No

CISA Form X (8/19) Page 8 of 42

 $[\]overline{^9}$ Providing these metrics enables CISA to prioritize unattributed cyber intrusions for further analysis.

INCIDENT REPORTING REQUIREMENTS					
72-HOUR INCIDENT UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITES COMPLETE) (CONTINUED)					
C. Identifying Techniques and Motivations (Continued)					
2. Strategic Direction Targeted intrusions against strategic targets? Yes No Specificity of data or information stolen or manipulated? Yes No Aligned with global or political event? Yes No Aligned with known foreign government policies? Yes No					
D. Estimating Publicity					
1. Is the government tracking this or similar incidents? 2. Is there national media coverage or other widely available public coverage? 3. Are foreign state adversaries tracking this incident? 4. Are foreign non-state adversaries tracking this incident? 5. Are discussions about the incident taking place in online communities? Yes No No					
6. Using the matrices from the MITRE ATT&CK™¹⁰ framework, list all adversarial tactics and techniques that relate to this incident below:					
A. If the incident involved Windows, Mac, or Linux platforms, utilize the Enterprise Matrix ¹¹ :					
B. If the incident involved access to a mobile device, utilize the Mobile Device Access Matrix ¹² :					
C. If the incident involved network-based effects, not necessarily linked to mobile device access, utilize the Mobile Network-Based Effects Matrix ¹³ :					
POST-INCIDENT UPDATE (WITHIN [7] DAYS OF RESOLUTION)					
The below elements are required (if available) when reporting to CISA:					
1. What information was needed sooner and from whom?					
What could CISA and the impacted organization do differently the next time a similar incident occurs to improve the incident handling process?					

CISA Form X (8/19) Page 9 of 42

^{0 2018} The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation and in accordance with the Terms of Use available here: https://attack.mitre.org/resources/terms-of-use/. CISA, DHS, or the U.S. Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA, DHS, or the U.S. Government.

¹¹ Information on tactics and techniques from the Enterprise Matrix can be found at https://attack.mitre.org/matrices/enterprise.

¹² Information on tactics and techniques from the Mobile Device Access Matrix can be found at https://attack.mitre.org/matrices/mobile.

¹³ Information on tactics and techniques from the Mobile Network-Based Effects Matrix can be found at https://attack.mitre.org/matrices/mobile.

INCIDENT REPORTING REQUIREMENTS						
POST-INCIDENT UPDATE (WITHIN [7] DAYS OF RESOLUTION) (CONTINUED)						
3. How could information sharing between CISA and the impacted organization have been improved?						
4. What defensive measures can be implemented to prevent similar incidents in the future?						
5. 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?						
7. Describe the recovery strategy used:						
8. Was the recovery strategy successful?						
8A. If unsuccessful, provide details on how the strategy was revised:						

CISA Form X (8/19) Page 10 of 42

MAJOR INCIDENT REPORTING REQUIREMENTS							
	ONE-HOUR MAJOR INCIDENT INITIAL REPORT						
	The below elements are <u>required</u> (if available) when reporting a major incident to the Cybersecurity and Infrastructure Security Agency (CISA) for the first time:						
1. Is this an update to a	previously	reported incide	nt? Yes	☐ No			
1A. If yes, please provid	e the incid	ent report and j	ustification:				
2. User Type: Impa	cted User	Reporting	on Behalf of the	Impacted User			
3. Name of Reporter							
A. First:		B. Middle (if a	pplicable):	C. Last:			D. Suffix (if applicable):
	Number(s		5. Preferred Er	mail Address of 0	Organiza	tion (i.e., soc@orga	nization.gov,
A. Unclassified:	B. Classi	fied:	soc@organi	zation.com):			
6. Top-Level Organization	on						
A. Name:				B. Type:			
C. Point(s) of Contact							
1. Name							
First:		Middle (if appli	icable):	Last:	Last:		Suffix (if applicable):
2 Phone	Number(s)			3 Fma	il Address	
Unclassified:	Classifie		Unclassified: Classified:				
7 Organization Sub Ent	its c			9 Critical Ir	ofrontruo	turo Soctor	
7. Organization Sub-Entity: 8. Critical Infrastructure Sector:							
9. Identify the current level of impact on agency functions or services (Functional Impact):							
10. Estimate the scope of time and resources needed to recover from the incident (Recoverability):							
11. On-site or remote as	sistance re	equired?					
Yes No If yes, identify:							
12. Are the impacted sys	tem(s) Fed	leral Information	n Security Moder	nization Act of 20	014 (FISI	MA) ¹⁴ system(s)? ¹⁵	
Yes No If yes, provide name of system(s):							
13. Is this a High Value	Asset?	14. When was	the activity first o	detected?			
15. What detection methods were used to discover this activity?							
Administrator Intrusion Detection System (IDS) User Other Anti-Virus Software Unknown							
16. What date and time was the incident declared? (Universal Time Coordinated [UTC] or local time with UTC offset)							
Date: Time:							

CISA Form X (8/19) Page 11 of 42

¹⁴ 44 U.S.C. §§ 3551-3558.

¹⁵ Pursuant to FISMA, an "information system" is defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

MAJOR INCIDENT REPORTING REQUIREMENTS							
ONE-HOUR MAJOR INCIDENT INITIAL REPORT							
17. How many of the following wer	e impacted?						
Systems							
Endpoints							
Operating SystemsServer Types							
Email File Print Web Cloud Kerberos TELNET Secure Shell (State Authors) Virtual Private N Domain Name S File Transfer Pro	SH) ority (CA) etwork (VPN) system (DNS)	Active Dire Voice over Security In Dynamic F Remote Lo Authentica (i.e., Radiu System [T.	ime Protocol (NTP) ectory (AD) Compon Internet Protocol (Volformation and Even Host Configuration P og(s) (i.e., Email, VP otion, Authorization, sus, Terminal Access ACACS+]) at Directory Access F otocol over Secure S	/oIP) Gateways t Management (SIE rotocol (DHCP) PN, Syslog, R-Syslog and Accounting (AA Controller Access-O	g, Syslog-NG) A) Services Control t Directory		
Network Devices							
		IDS Intrusion Protection S	System (IPS)	Load Balancers Hub	Other		
Users	_		_				
18. What network location(s) and information system(s) was the activity observed in?							
<i>、,</i>	·	,					
18A. What network segment(s) or Virtual Local Area Network(s) was the activity observed in?							
19. Describe the nature of the acti	vity:						
00 Dib	J-44J.						
20. Describe how the events were	detected:						
21. Have any actions been taken t		e you also reporting a					
recover from the major inciden Yes No	t? un ☐ Ye	authorized access to s	one or more persor refer to the breach	-	•		
23. Identify the points of contact and contact details for additional follow-up (a 24-hours per day, 7 days per week operations center point of contact is preferred).							
A. Name							
First:	Middle (if appl	cable):	Last:		Suffix (if applicable):		
B. Phone Number(s)		L C. Ema	il Address	<u> </u>		
Unclassified: Classifie		Unclassified:		Classified:			

CISA Form X (8/19) Page 12 of 42

MAJOR INCIDENT REPORTING REQUIREMENTS		
ONE-HOUR MAJOR INCIDENT INITIAL REPORT		
24. Did this major incident involve an unattributed cyber intru	sion?	
Yes No If yes, answer whether each of the follow	wing events was observed.16	
A. Understanding the Victim		
 Defense and Weapons Systems Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Financial Sector 	Yes No Yes No Yes No	
Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes No Yes No Yes No	
3. Government and Support Networks Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes No Yes No Yes No	
4. Health and Public Safety Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes No Yes No Yes No	
5. National Communications and Technology Infrastruct Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	rure	
6. Public Transportation Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes No Yes No Yes No	
7. Public Utilities Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes No Yes No Yes No	
B. Recognizing Impact and Effects		
1. Observed impact to domestic or foreign policy? 2. Observed impact to government operations? 3. Observed impact to national or global financial systems or economy? 4. Observed impact to intellectual property? 5. Observed impact to domestic or foreign reputation of governments or corporations? Yes No No		
C. Identifying Techniques and Motivations		
1. Sophistication Human-enabled or close-access operations? Complex delivery or exfiltration techniques? Custom, tailored, or unique tool(s) used? Complex obfuscation techniques? Established persistence?	Yes No Yes No Yes No Yes No Yes No	

CISA Form X (8/19) Page 13 of 42

¹⁶ Providing these metrics enables CISA to prioritize unattributed cyber intrusions for further analysis.

MAJOR INCIDENT REPORTING REQUIREMENTS		
ONE-HOUR MAJOR INCIDENT INITIAL REPORT		
C. Identifying Techniques and Motivations (Continued)		
2. Strategic Direction Targeted intrusions against strategic targets?		
D. Estimating Publicity		
1. Is the government tracking this or similar incidents? 2. Is there national media coverage or other widely available public coverage? 3. Are foreign state adversaries tracking this incident? 4. Are foreign non-state adversaries tracking this incident? 5. Are discussions about the incident taking place in online communities? Yes No No		
25. Using the matrices from the MITRE ATT&CK™¹7 framework, list all adversarial tactics and techniques that relate to this major incident below:		
A. If the major incident involved Windows, Mac, or Linux platforms, utilize the Enterprise Matrix ¹⁸ :		
B. If the major incident involved access to a mobile device, utilize the Mobile Device Access Matrix ¹⁹ :		
C. If the major incident involved network-based effects, not necessarily linked to mobile device access, utilize the Mobile Network-Based Effects Matrix ²⁰ :		
72-HOUR MAJOR INCIDENT UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITES COMPLETE)		
The below elements are <u>required</u> (if available) when reporting to CISA:		
On-site or remote assistance required?		
Yes No If yes, identify:		
2. Are you downgrading this from a major incident?		
2A. If yes, please provide justification:		

CISA Form X (8/19) Page 14 of 42

⁰²⁰¹⁸ The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation and in accordance with the Terms of Use available here: https://attack.mitre.org/resources/terms-of-use/. CISA, DHS, or the U.S. Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA, DHS, or the U.S. Government.

¹⁸ Information on tactics and techniques from the Enterprise Matrix can be found at https://attack.mitre.org/matrices/enterprise.

¹⁹ Information on tactics and techniques from the Mobile Device Access Matrix can be found at https://attack.mitre.org/matrices/mobile.

²⁰ Information on tactics and techniques from the Mobile Network-Based Effects Matrix can be found at https://attack.mitre.org/matrices/mobile.

MAJOR INCIDENT REPORTING REQUIREMENTS			
72-HOUR MAJOR INCIDENT UPDATE (CONTINUOUS UNTIL	ALL ERADICATION ACTIVITES COMPLETE) (CONTINUED)		
3. Are you also reporting a breach at this time (i.e., confirmed or poinformation records)?	otential unauthorized access to one or more personally identifiable		
Yes No If yes, refer to the breach reporting requirement	ents		
4. Substantive updates <u>required</u> , provide if available:			
A. Attack Vector(s):			
That led to the major incident:	Detected during the course of investigation:		
B. Indicators of Compromise (IOC):			
IOC:	Traffic Light Protocol Color:		
Indicator Title:	Indicator Description:		
IOC Kill-Chain Step:	Countermeasure(s):		
Should the cyber threat indicator or defensive measure contained in this submission be considered commercial, financial, and proprietary information submitted by a non-federal entity, as defined, to the U.S. Federal Government under the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. § 1504(d)(2))? Yes No			
4C. Domains Associated with the major incident:			
4D. Internet protocol (IP) addresses and their relation to the major			
4E. Malicious software or malicious scripts detected (by humans or Personal Security Products) via "Report Malware" on the United States Computer Emergency Readiness Team website:			
4F. Mitigation activities undertaken in response to the major incident:			
4G. Description of how the major incident occurred:			
4H. How the major incident was identified:			

CISA Form X (8/19) Page 15 of 42

MAJOR INCIDENT REPORTING REQUIREMENTS		
72-HOUR MAJOR INCIDENT UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITES COMPLETE) (CONTINUED)		
4I. How many of the following were impacted?		
Systems		
☐ Endpoints		
 □ Operating Systems □ Server Types □ Email □ File □ Active Directory (AD) Components □ Print □ Voice over Internet Protocol (VoIP) Gateways 		
Web Cloud Dynamic Host Configuration Protocol (DHCP) Kerberos TELNET Secure Shell (SSH) Remote Shell (RSH) Security Information and Event Management (SIEM) Dynamic Host Configuration Protocol (DHCP) Remote Log(s) (i.e., Email, VPN, Syslog, R-Syslog, Syslog-NG) Authentication, Authorization, and Accounting (AAA) Services (i.e., Radius, Terminal Access Controller Access-Control System [TACACS+])		
Certificate Authority (CA) Virtual Private Network (VPN) Domain Name System (DNS) File Transfer Protocol (FTP) Lightweight Directory Access Protocol/Lightweight Directory Access Protocol over Secure Sockets Layer (LDAP/LDAP[S]) Other		
Network Devices		
Routers Firewalls IDS Load Balancers Other Switches Proxies Intrusion Protection System (IPS) Hub Users		
4J. Based on the phase of the incident response process ²¹ , provide the following:		
Containment		
a. Strategy:		
b. As an update, was the containment strategy successful:		
c. If unsuccessful, provide details on how your strategy is changing:		
2. Eradication		
a. Strategy:		
b. As an update, was the eradication strategy successful:		
c. If unsuccessful, provide details on how your strategy is changing:		
4K. Provide upon request and if available (with the documentation or agreement to provisions as requested by CISA):1. Memory captures from information systems where threat actor activity was identified or suspected:		
1. Memory captures nom information systems where theat actor activity was identified or suspected.		

CISA Form X (8/19) Page 16 of 42

National Institute of Standards and Technology Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide. U.S. Department of Commerce. August 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

MAJOR INCIDENT REPORTING REQUIREMENTS			
	72-HOUR MAJOR INCIDENT UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITES COMPLETE) (CONTINUED)		
2.	2. System logs from compromised systems (starting from 24-hours prior to the first event identified in the major incident, through the present time):		
Αŗ	pplication:		
Sy	ystem Security:		
Ot	ther logs collected by the system(s) and/or application(s):		
	Network logs (starting from 24-hours prior to the first event communication from the impacted host(s). Logs include, but Hypervisor, Netflow, Network Device, Proxy, and HyperText	ut are not li	limited to: DHCP, DNS, Firewall, Packet Capture, Host,
4.	Provide a timeline of identified or suspected compromised but are not limited to: Source IP Address, Source Hostnam Destination IP Address, Destination Hostname, Destination Communication Start Time (UTC or local time with UTC of offset).	ne, Source n FQDN, D	Destination Port, Transport Protocol, Application Protocol,
5.	Did this incident involve an unattributed cyber intrusion?		
	Yes No If yes, answer whether each of the follow	wing event	its was observed. ²²
	. Understanding the Victim		
1.	Defense and Weapons Systems Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes Yes Yes	NoNoNoNo
2.	Financial Sector Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes Yes Yes	NoNoNoNo
3.	Government and Support Networks Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes Yes Yes	NoNoNoNo
4.	Health and Public Safety Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes Yes Yes	NoNoNoNo
5.	National Communications and Technology Infrastruct Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes Yes Yes	NoNoNoNo

CISA Form X (8/19) Page 17 of 42

 $[\]overline{^{22}}$ Providing these metrics enables CISA to prioritize unattributed cyber intrusions for further analysis.

MAJOR INCIDENT REPORTING REQUIREMENTS		
72-HOUR MAJOR INCIDENT UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITES COMPLETE) (CONTINUED)		
A. Understanding the Victim (Continued)		
6. Public Transportation Observed network intrusion or penetration?		
7. Public Utilities Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems? Yes No Observed access to control systems? Yes No		
B. Recognizing Impact and Effects		
1. Observed impact to domestic or foreign policy? 2. Observed impact to government operations? 3. Observed impact to national or global financial systems or economy? 4. Observed impact to intellectual property? 5. Observed impact to domestic or foreign reputation of governments or corporations? Yes No No		
C. Identifying Techniques and Motivations		
1. Sophistication Human-enabled or close-access operations?		
2. Strategic Direction Targeted intrusions against strategic targets? Specificity of data or information stolen or manipulated? Aligned with global or political event? Aligned with known foreign government policies? Yes No No		
D. Estimating Publicity		
1. Is the government tracking this or similar incidents? 2. Is there national media coverage or other widely available public coverage? 3. Are foreign state adversaries tracking this incident? 4. Are foreign non-state adversaries tracking this incident? 5. Are discussions about the incident taking place in online communities? Yes No No		
6. Using the matrices from the MITRE ATT&CK™²³ framework, list all adversarial tactics and techniques that relate to this major incident below:		
A. If the major incident involved Windows, Mac, or Linux platforms, utilize the Enterprise Matrix ²⁴ :		
B. If the major incident involved access to a mobile device, utilize the Mobile Device Access Matrix ²⁵ :		

CISA Form X (8/19) Page 18 of 42

²³© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation and in accordance with the Terms of Use available here: https://attack.mitre.org/resources/terms-of-use/. CISA, DHS, or the U.S. Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA, DHS, or the U.S. Government.

²⁴ Information on tactics and techniques from the Enterprise Matrix can be found at https://attack.mitre.org/matrices/enterprise.

²⁵ Information on tactics and techniques from the Mobile Device Access Matrix can be found at https://attack.mitre.org/matrices/mobile.

MAJOR INCIDENT REPORTING REQUIREMENTS

72-HOUR MAJOR INCIDENT UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITES COMPLETE) (CONTINUED)

72-HOUR MAJOR INCIDENT UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITES COMPLETE) (CONTINUED)
C. If the major incident involved network-based effects, not necessarily linked to mobile device access, utilize the Mobile Network-Based Effects Matrix ²⁶ :
DOCT MA LOD INCIDENT LIDDATE (MITHIN 17) DAVE OF DECOLUTION)
POST-MAJOR INCIDENT UPDATE (WITHIN [7] DAYS OF RESOLUTION)
The below elements are required (if available) when reporting to CISA:
1. What information was needed sooner and from whom?
What could CISA and the impacted organization do differently the next time a similar incident occurs to improve the incident handling process?
3. How could information sharing between CISA and the impacted organization have been improved?
4. What defensive measures can be implemented to prevent similar incidents in the future?
5. What precursors or indicators should be watched for in the future to detect similar incidents?
6. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

CISA Form X (8/19) Page 19 of 42

and techniques from the Mobile Network-Based Effects Matrix can be found at https://attack.mitre.org/matrices/mobile.

MAJOR INCIDENT REPORTING REQUIREMENTS
POST-MAJOR INCIDENT UPDATE (WITHIN [7] DAYS OF RESOLUTION) (CONTINUED)
7. Describe the recovery strategy used:
8. Was the recovery strategy successful?
8A. If unsuccessful, provide details on how the strategy was revised:
BREACH REPORTING REQUIREMENTS
ONE-HOUR BREACH INITIAL REPORT
The below elements are <u>required</u> (if available) when reporting a breach to CISA for the first time:
1. Identify the category of the breach ²⁷ :
2. Does this breach involve the loss of PII for 100,000 or more people? Yes No
2A. If no, is the breach likely to result in demonstrable harm to ²⁸ : 1. National security interests of the United States? 2. Foreign relations of the United States? 3. Economy of the United States? 4. Public confidence of the American people? 5. Civil liberties of the American people? 6. Public health and safety of the American people? 7 Yes No
3. If this breach constitutes a major incident, are you updating a previously-reported breach?
Yes No Not a Major Incident
3A. If yes, please provide the breach report and justification:

CISA Form X (8/19) Page 20 of 42

²⁷ Pursuant to the Office of Management and Budget Memorandum M-17-12, individuals with access to agencies' federal information and information systems are required to report a suspected or confirmed breach to the agency as soon as possible and without unreasonable delay. This includes a breach in any medium or form, including paper, oral, and electronic.

²⁸ Agencies should determine the level of impact of the incident by using the existing incident management process established in the National Institute of Standards and Technology Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*.

BREACH REPORTING REQUIREMENTS					
ONE-HOUR BREACH INITIAL REPORT (CONTINUED)					
4. User Type: Impacted User Reporting on Behalf of the Impacted User					
5. Name of Reporter					
A. First:	B. Middle (if	applicable):	C. Last:		D. Suffix (if applicable):
6. Phone Num			il Address of Organiza	ation (i.e., soc@orga	anization.gov,
A. Unclassified: B. Classified: soc@organization.com):					
8. Top-Level Organization					
A. Name: B. Type:					
C. Point(s) of Contact					
1. Name					
First:	Middle (if app	licable):	Last:		Suffix (if applicable):
2. Phone Num	ber(s)		 3. Ema	ail Address	
	ssified:	Unclassified:	0. 2	Classified:	
9. Organization Sub-Entity:			10. Critical Infrastru	10. Critical Infrastructure Sector:	
11. Identify the current level of	of impact on agency	functions or service	 es (Functional Impact):	:	
12. Has someone other than	an authorized user	accessed or potentia	ally accessed PII?	Yes No	
Alternately, has an author for an other-than-authoriz		, or potentially acce	ssed, information	Yes No	
12A. If yes to either question, accessed, by an unauth				have been accessed	d, or potentially
Identifying Numbers	onzed user or for ar	i unaumonzeu purp	ose.		
Social Security Number:			Taxpayer Identific	cation Number:	
Truncated or Partial Social Security Number:		Business Taxpayer Identification Number			
Driver's License Number:		(Sole Proprietor):			
License Plate Number:		Credit/Debit Card Number:			
Drug Enforcement Administration (DEA) Registration Number:		Business Credit Card Number (Sole Proprietor):			
File/Case ID Number:			Vehicle Identification Number:		
_	atient ID Number:		Business Vehicle (Sole Proprietor):	Identification Numb	per
Health Plan Beneficiary Number:		Personal Bank A			
Student ID Number:			Business Bank Account Number		
Federal Student Aid Num	Business Ban		(Sole Proprietor):		
Passport Number:			Personal Device	Identifiers or	
Alien Registration Numbe	r:		☐ Serial Numbers:		
Department of Defense (DoD) ID Number: _		Business Device Serial Numbers (
DoD Benefits Number:			Personal Mobile	Number:	
Employee Identification N	lumber:	_	☐ Business Mobile		_
Professional License Number:		(Sole Proprietor):			

CISA Form X (8/19) Page 21 of 42

BREACH REPORTING REQUIREMENTS ONE-HOUR BREACH INITIAL REPORT (CONTINUED) 12A. If yes to either question, provide known or approximate counts of all types of PII that have been accessed, or potentially accessed, by an unauthorized user or for an unauthorized purpose: **Biographical Information** Name (including nicknames): Group/Organization Membership: Military Service Information: Gender: Mother's Maiden Name: Race: Date of Birth (Day, Month, Year): Business Mailing Address (Sole Proprietor): Ethnicity: Business Phone or Fax Number Nationality: (Sole Proprietor): Country of Birth: Global Positioning System City or County of Birth: (GPS)/Location Data: Marital Status: Personal Email Address: Citizenship: Business Email Address: Immigration Status: ___ Employment Information: Religion/Religious Preference: Personal Financial Information (including loan information): Home Address: Business Financial Information (including Zip Code: loan information): Home Phone or Fax Number: Alias (i.e., username or screenname): Spouse Information: Education Information: Sexual Orientation: Resume or Curriculum Vitae: Children Information: Professional/Personal References: Biometrics, Distinguishing Features, and Characteristics Fingerprints: Height: Video Recording: Palm Prints: Photos: Vascular Scans: Voice/Audio Recording: ____ Retina/Iris Scans: Dental Profile: DNA Sample or Profile: Signatures: Scars, Marks, Tattoos: Hair Color: Weight: Eye Color: **Medical and Emergency Information** Medical/Health Information: Workers' Compensation Information: Mental Health Information: Patient ID Number: Emergency Contact Information: Disability Information:

CISA Form X (8/19) Page 22 of 42

BREACH REPORTING REQUIREMENTS			
ONE-HOUR BREACH INITIAL REPORT (CONTINUED)			
12A. If yes to either question, provide known or approximate counts of all types of PII that have been accessed, or potentially accessed, by an unauthorized user or for an unauthorized purpose:			
Device Information			
Device Settings or Preferences (i.e., security level, sharing options, ringtones): Cell Tower Records (i.e., logs, user location, time, etc.):			
Network Communications Data:			
Other Specific Information or File Types			
Taxpayer Information/Tax Return Information:	Health Information:		
Law Enforcement Information:	Case Files:		
Security Clearance/Background Check Information:	Personnel Files:		
Civil/Criminal History Information/Police Record:	Credit History Information:		
Academic and Professional Background Information:	Other:		
13. Provide known or approximate counts of all PII types that	have been manipulated, destroyed, or rendered unusable:		
Identifying Numbers			
Social Security Number:	Taxpayer Identification Number:		
Truncated or Partial Social Security Number:	Business Taxpayer Identification Number		
Driver's License Number:	(Sole Proprietor):		
License Plate Number:	Credit/Debit Card Number:		
Drug Enforcement Administration (DEA) Registration Number:	Business Credit Card Number (Sole Proprietor):		
File/Case ID Number:	Vehicle Identification Number:		
Patient ID Number:	Business Vehicle Identification Number (Sole Proprietor):		
Health Plan Beneficiary Number:	Personal Bank Account Number:		
Student ID Number:	☐ Business Bank Account Number		
Federal Student Aid Number:	└── (Sole Proprietor):		
Passport Number:	Personal Device Identifiers or		
Alien Registration Number:	☐ Serial Numbers:		
Department of Defense (DoD) ID Number:	Business Device Identifiers or Serial Numbers (Sole Proprietor):		
DoD Benefits Number:	Personal Mobile Number:		
Employee Identification Number:	Business Mobile Number		
Professional License Number:	(Sole Proprietor):		

CISA Form X (8/19) Page 23 of 42

BREACH REPORTING REQUIREMENTS		
ONE-HOUR BREACH	I INITIAL REPORT (CONTINUED)	
13. Provide known or approximate counts of all PII types that	t have been manipulated, destroyed, or rendered unusable:	
Biographical Information		
Name (including nicknames):	Group/Organization Membership:	
Gender:	Military Service Information:	
Race:	Mother's Maiden Name:	
Date of Birth (Day, Month, Year):	Business Mailing Address	
Ethnicity:	☐ (Sole Proprietor):	
Nationality:	Business Phone or Fax Number (Sole Proprietor):	
Country of Birth:	Global Positioning System	
City or County of Birth:	(GPS)/Location Data:	
Marital Status:	Personal Email Address:	
Citizenship:	Business Email Address:	
Immigration Status:	Employment Information:	
Religion/Religious Preference:	Personal Financial Information (including	
Home Address:	└── loan information):	
Zip Code:	Business Financial Information (including loan information):	
Home Phone or Fax Number:	Alias (i.e., username or screenname):	
Spouse Information:	Education Information:	
Sexual Orientation:	Resume or Curriculum Vitae:	
Children Information:	Professional/Personal References:	
Biometrics, Distinguishing Features, and Characteristics	<u> </u>	
Fingerprints:	Height:	
Palm Prints:	Video Recording:	
Vascular Scans:	Photos:	
Retina/Iris Scans:	Voice/Audio Recording:	
Dental Profile:	DNA Sample or Profile:	
Scars, Marks, Tattoos:	Signatures:	
Hair Color:	Weight:	
Eye Color:		
Medical and Emergency Information		
Medical/Health Information:	Workers' Compensation Information:	
Mental Health Information:	Patient ID Number:	
Disability Information:	Emergency Contact Information:	

CISA Form X (8/19) Page 24 of 42

BREACH REPORTING REQUIREMENTS		
ONE-HOUR BREACH INITIA	AL REPORT (CONTINUED)	
13. Provide known or approximate counts of all PII types that have	been manipulated, destroyed, or rendered unusable:	
Device Information		
Device Settings or Preferences (i.e., security level, sharing options, ringtones):	Cell Tower Records (i.e., logs, user location, me, etc.):	
Network Communications Data:		
Other Specific Information or File Types		
Taxpayer Information/Tax Return Information:	Health Information:	
Law Enforcement Information:	Case Files:	
Security Clearance/Background Check Information:	Personnel Files:	
Civil/Criminal History Information/Police Record:	Credit History Information:	
Academic and Professional Background Information:	Other:	
14. Was this PII observed on the Internet? Yes No If yes, provide:		
Domains:	Internet Protocol (IP) Address(es):	
MALE III A		
Website(s):	Social Media Platform(s):	
15. Estimate the scope of time and resources needed to recover fro	om the breach (Recoverability):	
16. On-site or remote assistance required?		
Yes No If yes, identify:		
17. Are the impacted system(s) Federal Information Security Modernization Act of 2014 (FISMA) ²⁹ system(s)? ³⁰		
Yes No If yes, provide name of system(s):		
18. Is this a High Value Asset? Yes No		
19. Is this activity associated with an already reported incident?	20. When was the activity first detected?	
Yes No If yes, provide:		
CISA Tracking Number:		
Organization Tracking Number:		
20A. Describe the nature of the activity:		

CISA Form X (8/19) Page 25 of 42

^{29 44} U.S.C. §§ 3551-3558.

30 Pursuant to FISMA, an "information system" is defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

BREACH REPORTING REQUIREMENTS				
ONE-HOUR BREACH INITIAL REPORT (CONTINUED)				
21. What detection methods were used to discover this activity?				
Administrator Intrusion Detection System (IDS) User Other Anti-Virus Software Unknown				
22. What date and time was the breach declared? (Universal Time Coordinated [UTC] or local time with UTC offset)				
Date: Time:				
23. Number of individuals impacted? 24. Were individuals notified? Yes No				
25. How were individuals notified?				
Email Short Message Service (SMS) Parcel Other (Specify):				
26. Has this been reported to Congress?				
Yes No If yes: Date/time reported (UTC or local time with UTC offset):				
Reported to point of contact:				
27. Were services provided? Yes No If provided, number of services:				
Identity Monitoring: Identity Theft Insurance:				
Credit Monitoring: Full-service identity counseling and remediation services:				
28. What network location(s) and information system(s) was the activity observed in?				
28A. What network segment(s) or VLAN(s) was the activity observed in?				
29. Describe the nature of the activity:				
30. Describe how the events were detected:				
31. Have any actions been taken to recover from the breach? Yes No				
32. Identify the points of contact and contact details for additional follow-up (a 24-hours per day, 7 days per week operations center point of contact is preferred).				
A. Name				
First: Middle (if applicable): Last: Suffix (if applicable):				
B. Phone Number(s) C. Email Address				
Unclassified: Classified: Unclassified: Classified:				

CISA Form X (8/19) Page 26 of 42

BREACH REPORTING REQUIREMENTS					
ONE-HOUR BREACH INITIAL REPORT (CONTINUED)					
33. Did this breach involve an unattributed cyber intrusion?					
Yes No If yes, answer whether each of the follow	wing events was observed. ³¹				
A. Understanding the Victim					
1. Defense and Weapons Systems Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	 Yes No Yes No Yes No 				
2. Financial Sector Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	YesNoYesNoYesNo				
3. Government and Support Networks Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes No Yes No Yes No				
4. Health and Public Safety Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	 Yes				
5. National Communications and Technology Infrastruct Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	ture				
6. Public Transportation Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes No Yes No Yes No				
7. Public Utilities Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes No Yes No Yes No				
B. Recognizing Impact and Effects					
1. Observed impact to domestic or foreign policy? 2. Observed impact to government operations? 3. Observed impact to national or global financial systems or economy? 4. Observed impact to intellectual property? 5. Observed impact to domestic or foreign reputation of governments or corporations? Yes No No					
C. Identifying Techniques and Motivations					
1. Sophistication Human-enabled or close-access operations? Complex delivery or exfiltration techniques? Custom, tailored, or unique tool(s) used? Complex obfuscation techniques? Established persistence?	Yes No Yes No Yes No Yes No Yes No				

CISA Form X (8/19) Page 27 of 42

³¹ Providing these metrics enables CISA to prioritize unattributed cyber intrusions for further analysis.

BREACH REPORTING REQUIREMENTS				
ONE-HOUR BREACH INITIAL REPORT (CONTINUED)				
C. Identifying Techniques and Motivations (Continued)				
2. Strategic Direction Targeted intrusions against strategic targets? Yes No Specificity of data or information stolen or manipulated? Yes No Aligned with global or political event? Yes No Aligned with known foreign government policies? Yes No				
D. Estimating Publicity				
1. Is the government tracking this or similar breaches? 2. Is there national media coverage or other widely available public coverage? 3. Are foreign state adversaries tracking this breach? 4. Are foreign non-state adversaries tracking this breach? 5. Are discussions about the breach taking place in online communities? Yes No Yes No				
34. Using the matrices from the MITRE ATT&CK™32 framework, list all adversarial tactics and techniques that relate to this breach below:				
A. If the breach involved Windows, Mac, or Linux platforms, utilize the Enterprise Matrix ³³ :				
B. If the breach involved access to a mobile device, utilize the Mobile Device Access Matrix ³⁴ :				
C. If the breach involved network-based effects, not necessarily linked to mobile device access, utilize the Mobile Network-Based Effects Matrix ³⁵ :				

CISA Form X (8/19) Page 28 of 42

^{© 2018} The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation and in accordance with the Terms of Use available here: https://attack.mitre.org/resources/terms-of-use/. CISA, DHS, or the U.S. Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA, DHS, or the U.S. Government.

³³ Information on tactics and techniques from the Enterprise Matrix can be found at https://attack.mitre.org/matrices/enterprise.

³⁴ Information on tactics and techniques from the Mobile Device Access Matrix can be found at https://attack.mitre.org/matrices/mobile.

³⁵ Information on tactics and techniques from the Mobile Network-Based Effects Matrix can be found at https://attack.mitre.org/matrices/mobile.

BREACH REPORTING REQUIREMENTS					
72-HOUR BREACH UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITIES COMPLETE)					
The below elements are required (if available) when reporting to CISA:					
1. Identify the category of the breach ³⁶ :	ally Identifiable Information (PII)				
Answer the following questions about the breach. If any of these ite incident and should be reported appropriately.	ems are answered "yes," then this breach constitutes a major				
2. Does this breach involve the loss of PII for 100,000 or more peo	ple? Yes No				
2A. If no, is the breach likely to result in demonstrable harm to ³⁷ : 1. National security interests of the United States?					
3. Have you previously declared this breach as a major incident?	Yes No				
3A. If yes, are you downgrading this from a major incident? 4. On-site or remote assistance required?	Yes No				
Yes No If yes, identify:					
5. Are you contracting out assistance for the reported breach? If yes, provide name of contracted entity(ies):	Yes No				
6. Is this breach now considered a major incident? Yes	No				
7. Is there a separate but related incident, per the FISMA definition	of "incident," that you need to report? Yes No				
8. Substantive updates <u>required</u> , provide if available:					
A. Attack Vector(s):					
That led to the incident:	Detected during the course of investigation:				
B. Indicators of Compromise (IOC):					
IOC:	Traffic Light Protocol Color:				
Indicator Title:	Indicator Description:				
IOC Kill-Chain Step:	Countermeasure(s):				
Should the cyber threat indicator or defensive measure contained in this submission be considered commercial, financial, and proprietary information submitted by a non-federal entity, as defined, to the U.S. Federal Government under the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. § 1504(d)(2))?					
8C. Domains associated with the breach:					

CISA Form X (8/19) Page 29 of 42

³⁶ Pursuant to the Office of Management and Budget Memorandum M-17-12, individuals with access to agencies' federal information and information systems are required to report a suspected or confirmed breach to the agency as soon as possible and without unreasonable delay. This includes a breach in any medium or form, including paper, oral, and electronic.

³⁷ Agencies should determine the level of impact of the incident by using the existing incident management process established in the National Institute of Standards and Technology Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*.

BREACH REPORTING REQUIREMENTS
72-HOUR BREACH UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITIES COMPLETE) (CONTINUED)
8D. Internet protocol (IP) addresses and their relation to the breach (such as attacker and victim):
8E. Malicious software or malicious scripts detected (by humans or Personal Security Products) via "Report Malware" on the United States Computer Emergency Readiness Team website:
8F. Mitigation activities undertaken in response to the breach:
8G. Description of how the breach occurred:
8H. How the breach was identified:
8J. Based on the phase of the incident response process ³⁸ , provide the following:
1. Containment a. Strategy:
a. Strategy.
b. As an update, was the containment strategy successful:
c. If unsuccessful, provide details on how your strategy is changing:
2. Eradication
a. Strategy:
b. As an update, was the eradication strategy successful:
c. If unsuccessful, provide details on how your strategy is changing:

CISA Form X (8/19) Page 30 of 42

National Institute of Standards and Technology Special Publication 800-61 Revision 2. *Computer Security Incident Handling Guide*. U.S. Department of Commerce. August 2012. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

BREACH REPORTING REQUIREMENTS			
72-HOUR BREACH UPDATE (CONTINUOUS UNTI	L ALL ERADICATION ACTIVITIES COMPLETE) (CONTINUED)		
8K. Provide upon request and if available (with the document			
Memory captures from information systems where threat a	actor activity was identified or suspected:		
System logs from compromised systems (starting from 24 present time):	-hours prior to the first event identified in the breach, through the		
Application:			
System Security:			
Other logs collected by the system(s) and/or application(s):			
communication from the impacted host(s). Logs include, b	nt identified in the incident, through the present time) detailing out are not limited to: DHCP, DNS, Firewall, Packet Capture, Host, ext Transfer Protocol/HyperText Transfer Protocol Secure:		
but are not limited to: Source IP Address, Source Hostnar Destination IP Address, Destination Hostname, Destination	d systems communicating with other systems. Network artifacts include, me, Source Fully Qualified Domain Name (FQDN), Source Port, on FQDN, Destination Port, Transport Protocol, Application Protocol, ffset), and Communication End Time (UTC or local time with UTC		
9. Did this breach involve an unattributed cyber intrusion?			
Yes No If yes, answer whether each of the following	owing events was observed. ³⁹		
A. Understanding the Victim			
1. Defense and Weapons Systems Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	☐ Yes☐ No☐ Yes☐ No☐ Yes☐ No		
2. Financial Sector Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	 Yes No Yes No Yes No 		
3. Government and Support Networks Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	 Yes No Yes No Yes No 		
4. Health and Public Safety Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	 Yes No Yes No Yes No 		

CISA Form X (8/19) Page 31 of 42

³⁹ Providing these metrics enables CISA to prioritize unattributed cyber intrusions for further analysis.

BREACH REPORTING REQUIREMENTS				
72-HOUR BREACH UPDATE (CONTINUOUS UNTIL	L ALL ERADICATION ACTIVITIES COMPLETE) (CONTINUED)			
A. Understanding the Victim (Continued)				
5. National Communications and Technology Infrastruct Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	ture			
6. Public Transportation Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	YesNoYesNoYesNo			
7. Public Utilities Observed network intrusion or penetration? Observed access to data storage or file systems? Observed access to control systems?	Yes			
B. Recognizing Impact and Effects				
 Observed impact to domestic or foreign policy? Observed impact to government operations? Observed impact to national or global financial systems or Observed impact to intellectual property? Observed impact to domestic or foreign reputation of government. 	Yes No			
C. Identifying Techniques and Motivations				
1. Sophistication Human-enabled or close-access operations? Complex delivery or exfiltration techniques? Custom, tailored, or unique tool(s) used? Complex obfuscation techniques? Established persistence?	Yes No Yes No Yes No Yes No Yes No			
2. Strategic Direction Targeted intrusions against strategic targets? Specificity of data or information stolen or manipulated? Aligned with global or political event? Aligned with known foreign government policies?	Yes No Yes No Yes No Yes No			
D. Estimating Publicity				
1. Is the government tracking this or similar breaches? 2. Is there national media coverage or other widely available public coverage? 3. Are foreign state adversaries tracking this breach? 4. Are foreign non-state adversaries tracking this breach? 5. Are discussions about the breach taking place in online communities? Yes No No				
below:	ork, list all adversarial tactics and techniques that relate to this breach			
A. If the breach involved Windows, Mac, or Linux platforms, to	utilize the Enterprise Matrix ⁴¹ :			

CISA Form X (8/19) Page 32 of 42

⁴⁰ © 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation and in accordance with the Terms of Use available here: https://attack.mitre.org/resources/terms-of-use/. CISA, DHS, or the U.S. Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA, DHS, or the U.S. Government.

Information on tactics and techniques from the Enterprise Matrix can be found at https://attack.mitre.org/matrices/enterprise.

BREACH REPORTING REQUIREMENTS				
72-HOUR BREACH UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITIES COMPLETE) (CONTINUED)				
B. If the breach involved access to a mobile device, utilize the Mobile Device Access Matrix ⁴² :				
C. If the breach involved network-based effects, not necessarily linked to mobile device access, utilize the Mobile Network-Based Effects Matrix ⁴³ :				
POST-BREACH UPDATE (WITHIN [7] DAYS OF RESOLUTION)				
The below elements are required (if available) when reporting to CISA:				
What sould CISA and the impacted organization do differently the payt time a similar broach accurs to improve the broach.				
2. What could CISA and the impacted organization do differently the next time a similar breach occurs to improve the breach handling process?				
3. How could information sharing between CISA and the impacted organization have been improved?				
4. What defensive measures can be implemented to prevent similar breaches in the future?				

CISA Form X (8/19) Page 33 of 42

⁴³ Information on tactics and techniques from the Mobile Device Access Matrix can be found at https://attack.mitre.org/matrices/mobile.

43 Information on tactics and techniques from the Mobile Network-Based Effects Matrix can be found at https://attack.mitre.org/matrices/mobile.

BREACH REPORTING REQUIREMENTS					
POST	-BREACH UPDA	TE (WITHIN [7] DAY	S OF RESOLUTION	I) (CONTINUED)	
5. What precursors or indicators					
6. What additional tools or reso		to detect, analyze, a	nd mitigate future bre	aches?	
7. Describe the recovery strateon					
8. Was the recovery strategy su	_	es No			
8A. If unsuccessful, provide details on how the strategy was revised:					
EVENTS UNDER INVESTIGATION REPORTING					
	72-HOUR EVENT	S UNDER INVESTI	GATION INITIAL RE	PORTING	
The below elements are strong	y recommended w	vhen reporting an eve	ent under investigation	on for 72 hours to C	ISA for the first time:
1. User Type: Impacted Us	er Reporting	g on Behalf of the Imp	pacted User		
2. Name of Reporter					
A. First:	B. Middle (if a	applicable):	C. Last:		D. Suffix (if applicable):
	r(s) issified:	4. Preferred Email soc@organizatio	Address of Organiza on.com):	ition (i.e., soc@orga	anization.gov,
5. Top-Level Organization			Typo:		
A. Name:		B.	Type:		

CISA Form X (8/19) Page 34 of 42

EVENTS UNDER INVESTIGATION REPORTING						
72-HOUR EVENTS UNDER INVESTIGATION INITIAL REPORTING (CONTINUED)						
C. Point(s) of Contact						
1. Name						
First:		Middle (if appli	cable):	Last:		Suffix (if applicable):
	Number(s			3. Ema	il Address	
Unclassified:	Classifie	d:	Unclassified:		Classified:	
6. Organization Sub-Ent	ity:			7. Critical Infrastruc	ture Sector:	
8. Identify the current lev	vel of impa	ct on agency fu	nctions or service	s (Functional Impact):		
9. Estimate the scope of	time and	resources need	ed to recover fron	n the event (Recoverab	ility):	
10. On-site or remote as	sistance re	equired?				
Yes No If y	es, identify	<i>r</i> :				
11. Are the impacted sys	stem(s) Fed	deral Information	Security Modern	ization Act of 2014 (FIS	MA) ⁴⁴ system(s)? ⁴⁵	
Yes No If yes	s, provide	name of system	n(s):			
12. Is this a High Value	Asset?	13. When was	the activity first de	tected?		
Yes No						
14. What detection meth			-			
Administrator Intrusion Detection System (IDS) User Other Anti-Virus Software Log Review Unknown						
15. What date and time	was the in	cident declared	? (Universal Time	Coordinated [UTC] or I	ocal time with UTC	offset)
Date: Time:						
16. How many of the following were impacted? Systems						
☐ Endpoints						
☐ Operating Systems ☐ Server Types						
Email Network Time Protocol (NTP) File Active Directory (AD) Components Print Voice over Internet Protocol (VoIP) Gateways Security Information and Event Management (SIEM) Dynamic Host Configuration Protocol (DHCP) Kerberos Remote Log(s) (i.e., Email, VPN, Syslog, R-Syslog, Syslog-NG) Authentication, Authorization, and Accounting (AAA) Services (i.e., Radius, Terminal Access Controller Access-Control System [TACACS+]) Certificate Authority (CA) Virtual Private Network (VPN) Domain Name System (DNS) File Transfer Protocol (FTP)						

CISA Form X (8/19) Page 35 of 42

⁴⁴ 44 U.S.C. §§ 3551-3558.

⁴⁵ Pursuant to FISMA, an "information system" is defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

EVENTS UNDER INVESTIGATION REPORTING					
72-HOUR EVENTS UNDER INVESTIGATION INITIAL REPORTING (CONTINUED)					
16. How many of the following we	ere impacted? (C	Continued)			
Network Devices					
	irewalls	IDS Intrusion Protection	System (IPS)	Load Balancers Hub	Other
Users					
17. What network location(s) and	information sys	tem(s) was the activit	y observed in?		
17A. What network segment(s) o	r Virtual Local A	rea Network(s) was th	ne activity observed	in?	
• ()		, ,	·		
18. Describe the nature of the ac	ivitv:				
	, .				
19. Describe how the events wer	a detected:				
To. Bosonbo now the events wer	o dotootod.				
20. Identify the points of contact a point of contact is preferred).	and contact deta	ils for additional follo	w-up (a 24-hours pe	r day, 7 days per we	eek operations center
A. Name					
First:	Middle (if app	licable):	Last:		Suffix (if applicable):
B. Phone Number	s)		C. Em	ail Address	
Unclassified: Classifi	·	Unclassified:		Classified:	
04. D					
21. Provide if available:A. Domains associated with the example.	wont				
A. Domains associated with the e	vent.				
B. Internet protocol (IP) addresse	s and their relat	ion to the event (such	n as attacker and vic	tim):	
C Malicious software or maliciou	e scrints datacte	ad (by humans or Per	sonal Security Produ	ucts) via "Report Ma	lware" on the United
C. Malicious software or malicious scripts detected (by humans or Personal Security Products) via "Report Malware" on the United States Computer Emergency Readiness Team website:					
22. Provide, if available and applicable:					
A. Attack Vector(s) detected during the course of investigation:					

CISA Form X (8/19) Page 36 of 42

EVENTS UNDER INVESTIGATION REPORTING				
72-HOUR EVENTS UNDER INVESTIGATION INITIAL REPORTING (CONTINUED)				
B. Indicators of Compromise (IOC):				
IOC:	Traffic Light Protocol Color:			
Indicator Title:	Indicator Description:			
IOC Kill-Chain Step:	Countermeasure(s):			
Should the cyber threat indicator or defensive measure contained proprietary information submitted by a non-federal entity, as define Information Sharing Act of 2015 (6 U.S.C. § 1504(d)(2))? Yes	ed, to the U.S. Federal Government under the Cybersecurity			
23. Provide upon request and if available (with the documentation	or agreement to provisions as requested by CISA):			
A. Memory captures from information systems where threat actor a	activity was identified or suspected:			
B. System logs from compromised systems (starting from 24-hours present time):	s prior to the first event identified in the breach, through the			
Application:				
System Security:				
Other logs collected by the system(s) and/or application(s):				
C. Network logs (starting from 24-hours prior to the first event iden communication from the impacted host(s). Logs include, but are Hypervisor, Netflow, Network Device, Proxy, and HyperText Tra	not limited to: DHCP, DNS, Firewall, Packet Capture, Host,			
D. Provide a timeline of identified or suspected compromised systems communicating with other systems. Network artifacts include, but are not limited to: Source IP Address, Source Hostname, Source Fully Qualified Domain Name (FQDN), Source Port, Destination IP Address, Destination Hostname, Destination FQDN, Destination Port, Transport Protocol, Application Protocol, Communication Start Time (UTC or local time with UTC offset), and Communication End Time (UTC or local time with UTC offset).				
24. Using the matrices from the MITRE ATT&CK™ ⁴⁶ framework, list all adversarial tactics and techniques that relate to this event below:				
A. If the event involved Windows, Mac, or Linux platforms, utilize the	ne Enterprise Matrix ⁴⁷ :			

CISA Form X (8/19) Page 37 of 42

⁴⁶ © 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation and in accordance with the Terms of Use available here: https://attack.mitre.org/resources/terms-of-use/. CISA, DHS, or the U.S. Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA, DHS, or the U.S. Government.

⁴⁷ Information on tactics and techniques from the Enterprise Matrix can be found at https://attack.mitre.org/matrices/enterprise.

EVENTS UNDER INVESTIGATION REPORTING							
72-HOUR EVENTS UNDER INVESTIGATION INITIAL REPORTING (CONTINUED)							
B. If the event involved a	access to a	mobile device,	utilize the Mobil	e Device Access Matrix⁴	18.		
C. If the event involved r Effects Matrix ⁴⁹ :	network-ba	sed effects, not	t necessarily link	ed to mobile device acce	ess, utilize the Mobi	le Network-Based	
	(CO			NIVESTIGATION UPDA ICATION ACTIVITIES C			
The below elements are	strongly re	commended w	hen reporting to	CISA:			
1. User Type: Impac	cted User	Reporting	on Behalf of the	Impacted User			
2. Name of Reporter							
A. First:	A. First: B. Middle (if a		oplicable):	plicable): C. Last:		D. Suffix (if applicable):	
3. Phone Number(s) A. Unclassified: B. Classified:		4. Preferred Email Address of Organization (i.e., soc@organization.gov, soc@organization.com):					
5. Top-Level Organization	n						
A. Name:				В. Туре:			
C. Point(s) of Contact							
1. Name							
First:		Middle (if appli	cable):	Last:		Suffix (if applicable):	
2. Phone Number(s)			3. Ema	il Address			
Unclassified: Classified:		Unclassified: Classified:					
6. Organization Sub-Entity:				7. Critical Infrastructure Sector:			
8. Identify the current lev	el of impa	ct on agency fu	nctions or servic	es (Functional Impact):			
9. Estimate the scope of	time and r	esources need	ed to recover fro	m the event (Recoverab	ility):		
10. On-site or remote assistance required?							
Yes No If ye	es, identify	:					

CISA Form X (8/19) Page 38 of 42

⁴⁸ Information on tactics and techniques from the Mobile Device Access Matrix can be found at https://attack.mitre.org/matrices/mobile.

49 Information on tactics and techniques from the Mobile Network-Based Effects Matrix can be found at https://attack.mitre.org/matrices/mobile.

EVENTS UNDER INVESTIGATION REPORTING							
72-HOUR EVENTS UNDER INVESTIGATION UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITIES COMPLETE) (CONTINUED)							
11. Are the impacted system(s) Federal Information Security Modernization Act of 2014 (FISMA) ⁵⁰ system(s)? ⁵¹							
Yes No If yes, provide name of system(s):							
12. Is this a High Value Asset? 13. When was the activity first detected?							
☐ Yes ☐ No							
14. What detection methods were used to discover this activity?							
Administrator Intrusion Detection System (IDS) User Other Anti-Virus Software Unknown							
15. What date and time was the incident declared? (Universal Time Coordinated [UTC] or local time with UTC offset)							
Date: Time:							
16. How many of the following were impacted? Systems							
☐ Endpoints							
□ Operating Systems Server Types □ Email □ Active Directory (AD) Components □ Print □ Voice over Internet Protocol (VoIP) Gateways □ Web □ Security Information and Event Management (SIEM) □ Cloud □ Dynamic Host Configuration Protocol (DHCP) □ Kerberos □ Remote Log(s) (i.e., Email, VPN, Syslog, R-Syslog, Syslog-NG) □ TELNET Authentication, Authorization, and Accounting (AAA) Services □ Secure Shell (RSH) □ (i.e., Radius, Terminal Access Controller Access-Control □ Remote Shell (RSH) System [TACACS+]) □ Certificate Authority (CA) □ Lightweight Directory Access Protocol/Lightweight Directory Access Protocol over Secure Sockets Layer (LDAP/LDAP[S]) □ Domain Name System (DNS) □ Other □ Network Devices □ Routers □ Firewalls □ IDS □ Routers □ Firewalls □ Load Balancers □ Other							
Users							
17. What network location(s) and information system(s) was the activity observed in?							
17. What hetwork location(5) and information system(5) was the activity observed in:							
17A. What network segment(s) or Virtual Local Area Network(s) was the activity observed in?							
40. Describe the matrix of the set it.							
18. Describe the nature of the activity:							

Page 39 of 42 CISA Form X (8/19)

⁵⁰ 44 U.S.C. §§ 3551-3558.
⁵¹ Pursuant to FISMA, an "information system" is defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Page 39

EVENTS UNDER INVESTIGATION REPORTING										
72-HOUR EVENTS UNDER INVESTIGATION UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITIES COMPLETE) (CONTINUED)										
19. Describe how the events were detected:										
20. Have any actions been taken to recover from the event?										
21. Identify the points of contact and contact details for additional follow-up (a 24-hours per day, 7 days per week operations center point of contact is preferred).										
A. Name										
First: Middle		Middle (if appli	icable):	Last:		Suffix (if applicable):				
	Number(s			C. Ema	ail Address	1				
Unclassified:	assified: Classified:		Unclassified:		Classified:					
22. Provide if available:										
A. Domains associated was a special decorated by the second	addresses malicious ergency Re	and their relation	d (by humans or Pers			llware" on the United				
23. Provide, if available										
A. Attack Vector(s) dete	cted during	j the course of i	investigation:							
B. Indicators of Compro	mise (IOC)	:								
IOC:			Tra	affic Light Protocol (Color:					
Indicator Title:	dicator Title: Indicator Description:									
IOC Kill-Chain Step: Countermeasure(s):										
Should the cyber threat proprietary information s Information Sharing Act	ubmitted b	y a non-federal	l entity, as defined, to							

CISA Form X (8/19) Page 40 of 42

EVENTS UNDER INVESTIGATION REPORTING

=0.11011D EVENTO UNDER INVESTIGATION URBATE

(CONTINUOUS UNTIL ALL ERADICATION ACTIVITIES COMPLETE) (CONTINUED)
24. Provide upon request and if available (with the documentation or agreement to provisions as requested by CISA):
A. Memory captures from information systems where threat actor activity was identified or suspected:
B. System logs from compromised systems (starting from 24-hours prior to the first event identified in the breach, through the present time):
Application:
System Security:
Other logs collected by the system(s) and/or application(s):
C. Network logs (starting from 24-hours prior to the first event identified in the incident, through the present time) detailing communication from the impacted host(s). Logs include, but are not limited to: DHCP, DNS, Firewall, Packet Capture, Host, Hypervisor, Netflow, Network Device, Proxy, and HyperText Transfer Protocol/HyperText Transfer Protocol Secure:
D. Provide a timeline of identified or suspected compromised systems communicating with other systems. Network artifacts include, but are not limited to: Source IP Address, Source Hostname, Source Fully Qualified Domain Name (FQDN), Source Port, Destination IP Address, Destination Hostname, Destination FQDN, Destination Port, Transport Protocol, Application Protocol, Communication Start Time (UTC or local time with UTC offset), and Communication End Time (UTC or local time with UTC offset).
25. Using the matrices from the MITRE ATT&CK™52 framework, list all adversarial tactics and techniques that relate to this event below:
A. If the event involved Windows, Mac, or Linux platforms, utilize the Enterprise Matrix ⁵³ :

CISA Form X (8/19) Page 41 of 42

⁵² © 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation and in accordance with the Terms of Use available here: https://attack.mitre.org/resources/terms-of-use/. CISA, DHS, or the U.S. Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA, DHS, or the U.S. Government.

Information on tactics and techniques from the Enterprise Matrix can be found at https://attack.mitre.org/matrices/enterprise.

T2-HOUR EVENTS UNDER INVESTIGATION UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITIES COMPLETE) (CONTINUED) B. If the event involved access to a mobile device, utilize the Mobile Device Access Matrix⁵⁴: C. If the event involved network-based effects, not necessarily linked to mobile device access, utilize the Mobile Network-Based Effects Matrix⁴⁹:

CISA Form X (8/19) Page 42 of 42

⁵⁴ Information on tactics and techniques from the Mobile Device Access Matrix can be found at https://attack.mitre.org/matrices/mobile.

⁵⁵ Information on tactics and techniques from the Mobile Network-Based Effects Matrix can be found at https://attack.mitre.org/matrices/mobile.