DEPARTMENT OF HOMELAND SECURITY
Cybersecurity and Infrastructure Security Agency

OMB Control No: 1670-0037
Expiration Date: 12/31/2021

INCIDENT REPORTING FORM

PURPOSE: 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 **not** add sensitive personally identifiable information (SPII) to incident submissions. Any contact information collected will be handled according to the **Department of Homeland Security (DHS) privacy policies.**

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 BASICS

View the updated FIRR requirements for descriptions of the different reporting categories.

1. Are you reporting an incident, major incident, breach, or Event under Investigation at this time?

☐ Incident ☐ Major Incident ☐ Breach ☐ Event Under Investigation

2. What type of report are you submitting?

☐ One-Hour Initial Report ☐ 72-Hour Initial Report ☐ 72-Hour Update ☐ Post Incident/Major Incident Breach Update

INCIDENT REPORTING REQUIREMENTS

ONE-HOUR INITIAL INCIDENT REPORT

The below elements are required (if available) when reporting an incident to CISA for the first time:

1. User Type: ☐ Impacted User ☐ Reporting on Behalf of the Impacted User

2. Name of Reporter

A. First:	B. Middle (if applicable):	C. Last:	D. Suffix (if applicable):

3. Phone Number(s)		4. Preferred Email Address of Organization (i.e., soc@organization.gov, soc@organization.com):
A. Unclassified:	B. Classified:	

5. Top-Level Organization

A. Name:	B. Type:

C. Point(s) of Contact

1. Name

First:	Middle (if applicable):	Last:	Suffix (if applicable):

2. Phone Number(s)		3. Email Address	
Unclassified:	Classified:	Unclassified:	Classified:

6. Organization Sub-Entity:	7. Critical Infrastructure Sector:

8. Identify the current level of impact on agency functions or services (Functional Impact):

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?

☐ Yes ☐ No

13. When was the activity first detected?

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
☐ 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 ☐ Load Balancers ☐ Other
☐ Switches ☐ Proxies ☐ Intrusion Protection System (IPS) ☐ Hub

☐ Users

[1] 44 U.S.C. §§ 3551-3558.

[2] 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 Virtual Local Area Network(s) was the activity observed in?

18. Describe the nature of the activity:

19. Describe how the events were detected:

20. Have any actions been taken to recover from the incident?
☐ Yes ☐ No

21. Are you also reporting a breach at this time (i.e., confirmed or potential unauthorized access to one or more personally identifiable information records)?
☐ Yes ☐ No If yes, refer to the breach reporting requirements

22. 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:

23. Did this incident involve an unattributed cyber intrusion?

☐ Yes ☐ No If yes, answer whether each of the following events was observed.[3]

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? ☐ Yes ☐ No
- Observed access to data storage or file systems? ☐ Yes ☐ No
- Observed access to control systems? ☐ Yes ☐ No

3. Government and Support Networks
- Observed network intrusion or penetration? ☐ Yes ☐ No
- Observed access to data storage or file systems? ☐ Yes ☐ No
- Observed access to control systems? ☐ Yes ☐ No

4. Health and Public Safety
- Observed network intrusion or penetration? ☐ Yes ☐ No
- Observed access to data storage or file systems? ☐ Yes ☐ No
- Observed access to control systems? ☐ Yes ☐ No

5. National Communications and Technology Infrastructure
- Observed network intrusion or penetration? ☐ Yes ☐ No
- Observed access to data storage or file systems? ☐ Yes ☐ No
- Observed access to control systems? ☐ Yes ☐ No

[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?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

7. Public Utilities

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

B. Recognizing Impact and Effects

1. Observed impact to domestic or foreign policy?	☐ Yes	☐ No
2. Observed impact to government operations?	☐ Yes	☐ No
3. Observed impact to national or global financial systems or economy?	☐ Yes	☐ No
4. Observed impact to intellectual property?	☐ Yes	☐ No
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?	☐ Yes	☐ No
Complex delivery or exfiltration techniques?	☐ Yes	☐ No
Custom, tailored, or unique tool(s) used?	☐ Yes	☐ No
Complex obfuscation techniques?	☐ Yes	☐ No
Established persistence?	☐ Yes	☐ No

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?	☐ Yes	☐ No
2. Is there national media coverage or other widely available public coverage?	☐ Yes	☐ No
3. Are foreign state adversaries tracking this incident?	☐ Yes	☐ No
4. Are foreign non-state adversaries tracking this incident?	☐ Yes	☐ No
5. Are discussions about the incident taking place in online communities?	☐ Yes	☐ 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]:

[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 INCIDENT REPORT (CONTINUED)

B. If the incident involved access to a mobile device, utilize the Mobile Device Access Matrix[6]:

C. If the incident involved network-based effects, not necessarily linked to mobile device access, utilize the Mobile Network-Based Effects Matrix[7]:

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

The below elements are required (if available) when reporting to CISA:

1. On-site or remote assistance required?

☐ Yes ☐ No If yes, identify: _____

2. Are you upgrading this incident to a major incident? ☐ Yes ☐ No

2A. If yes, please provide justification:

3. Are you also reporting a breach at this time (i.e., confirmed or potential unauthorized access to one or more personally identifiable information records)?

☐ Yes ☐ No If yes, refer to the breach reporting requirements

4. Substantive updates required, 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))? ☐ Yes ☐ No

4C. Domains Associated with the Incident:

[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 UNTIL ALL ERADICATION ACTIVITES COMPLETE) (CONTINUED)

4D. Internet protocol (IP) addresses and their relation to the incident (such as attacker and victim):

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 incident:

4G. Description of how the incident occurred:

4H. How the incident was identified:

4I. How many of the following were impacted?

- ☐ Systems
  - ☐ Endpoints
    - ☐ Operating Systems
    - ☐ Server 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
    - ☐ Switches
    - ☐ Firewalls
    - ☐ Proxies
    - ☐ IDS
    - ☐ Intrusion Protection System (IPS)
    - ☐ Load Balancers
    - ☐ Hub
    - ☐ Other
- ☐ Users

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:
1. 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:
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).

[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.

INCIDENT REPORTING REQUIREMENTS

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

5. Did this incident involve an unattributed cyber intrusion?

☐ Yes ☐ No If yes, answer whether each of the following events was observed.[9]

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?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

3. Government and Support Networks

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

4. Health and Public Safety

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

5. National Communications and Technology Infrastructure

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

6. Public Transportation

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

7. Public Utilities

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

B. Recognizing Impact and Effects

1. Observed impact to domestic or foreign policy?	☐ Yes	☐ No
2. Observed impact to government operations?	☐ Yes	☐ No
3. Observed impact to national or global financial systems or economy?	☐ Yes	☐ No
4. Observed impact to intellectual property?	☐ Yes	☐ No
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?	☐ Yes	☐ No
Complex delivery or exfiltration techniques?	☐ Yes	☐ No
Custom, tailored, or unique tool(s) used?	☐ Yes	☐ No
Complex obfuscation techniques?	☐ Yes	☐ No
Established persistence?	☐ Yes	☐ No

[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?	☐ Yes	☐ No
2. Is there national media coverage or other widely available public coverage?	☐ Yes	☐ No
3. Are foreign state adversaries tracking this incident?	☐ Yes	☐ No
4. Are foreign non-state adversaries tracking this incident?	☐ Yes	☐ No
5. Are discussions about the incident taking place in online communities?	☐ Yes	☐ 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?

2. What could CISA and the impacted organization do differently the next time a similar incident occurs to improve the incident handling process?

[10] © 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?
6. 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? ☐ Yes ☐ No
8A. If unsuccessful, provide details on how the strategy was revised:

MAJOR INCIDENT REPORTING REQUIREMENTS

ONE-HOUR MAJOR INCIDENT INITIAL REPORT

The below elements are required (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 incident? ☐ Yes ☐ No

1A. If yes, please provide the incident report and justification:

2. User Type: ☐ Impacted User ☐ Reporting on Behalf of the Impacted User

3. Name of Reporter

A. First:	B. Middle (if applicable):	C. Last:	D. Suffix (if applicable):

4. Phone Number(s)		5. Preferred Email Address of Organization (i.e., soc@organization.gov, soc@organization.com):
A. Unclassified:	B. Classified:	

6. Top-Level Organization

A. Name:	B. Type:

C. Point(s) of Contact

1. Name

First:	Middle (if applicable):	Last:	Suffix (if applicable):

2. Phone Number(s)		3. Email Address	
Unclassified:	Classified:	Unclassified:	Classified:

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 assistance required?

☐ Yes ☐ No If yes, identify: _____

12. Are the impacted system(s) Federal Information Security Modernization Act of 2014 (FISMA)[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 detected?
☐ Yes ☐ No	

15. What detection methods were used to discover this activity?

☐ Administrator ☐ Intrusion Detection System (IDS) ☐ User ☐ Other
☐ Anti-Virus Software ☐ Log Review ☐ Unknown

16. What date and time was the incident declared? (Universal Time Coordinated [UTC] or local time with UTC offset)

Date: _____ Time: _____

[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 were impacted?

- ☐ Systems
  - ☐ Endpoints
    - ☐ Operating Systems
    - ☐ Server 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 ☐ Load Balancers ☐ Other
    - ☐ Switches ☐ Proxies ☐ Intrusion Protection System (IPS) ☐ Hub
- ☐ Users

18. What network location(s) and information system(s) was the activity observed in?

18A. What network segment(s) or Virtual Local Area Network(s) was the activity observed in?

19. Describe the nature of the activity:

20. Describe how the events were detected:

21. Have any actions been taken to recover from the major incident?	22. Are you also reporting a breach at this time (i.e., confirmed or potential unauthorized access to one or more personally identifiable information records)?
☐ Yes ☐ No	☐ Yes ☐ No If yes, refer to the breach reporting requirements

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 applicable):	Last:	Suffix (if applicable):

B. Phone Number(s)		C. Email Address	
Unclassified:	Classified:	Unclassified:	Classified:

MAJOR INCIDENT REPORTING REQUIREMENTS

ONE-HOUR MAJOR INCIDENT INITIAL REPORT

24. Did this major incident involve an unattributed cyber intrusion?

☐ Yes ☐ No If yes, answer whether each of the following events was observed.[16]

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?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

3. Government and Support Networks

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

4. Health and Public Safety

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

5. National Communications and Technology Infrastructure

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

6. Public Transportation

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

7. Public Utilities

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

B. Recognizing Impact and Effects

1. Observed impact to domestic or foreign policy?	☐ Yes	☐ No
2. Observed impact to government operations?	☐ Yes	☐ No
3. Observed impact to national or global financial systems or economy?	☐ Yes	☐ No
4. Observed impact to intellectual property?	☐ Yes	☐ No
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?	☐ Yes	☐ No
Complex delivery or exfiltration techniques?	☐ Yes	☐ No
Custom, tailored, or unique tool(s) used?	☐ Yes	☐ No
Complex obfuscation techniques?	☐ Yes	☐ No
Established persistence?	☐ Yes	☐ No

[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?	☐ 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?	☐ Yes	☐ No
2. Is there national media coverage or other widely available public coverage?	☐ Yes	☐ No
3. Are foreign state adversaries tracking this incident?	☐ Yes	☐ No
4. Are foreign non-state adversaries tracking this incident?	☐ Yes	☐ No
5. Are discussions about the incident taking place in online communities?	☐ Yes	☐ 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 required (if available) when reporting to CISA:

1. On-site or remote assistance required?

☐ Yes ☐ No If yes, identify: _____

2. Are you downgrading this from a major incident? ☐ Yes ☐ No

2A. If yes, please provide justification:

[17] © 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.

[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 potential unauthorized access to one or more personally identifiable information records)? ☐ Yes ☐ No If yes, refer to the breach reporting requirements	
4. Substantive updates required, 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 incident (such as attacker and victim):	
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:	

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
      - ☐ 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 ☐ 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:

1. 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:

[21] 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. System logs from compromised systems (starting from 24-hours prior to the first event identified in the major 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 major 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).

5. Did this incident involve an unattributed cyber intrusion?

☐ Yes ☐ No If yes, answer whether each of the following events was observed.[22]

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?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

3. Government and Support Networks

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

4. Health and Public Safety

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

5. National Communications and Technology Infrastructure

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

[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?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

7. Public Utilities

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

B. Recognizing Impact and Effects

1. Observed impact to domestic or foreign policy?	☐ Yes	☐ No
2. Observed impact to government operations?	☐ Yes	☐ No
3. Observed impact to national or global financial systems or economy?	☐ Yes	☐ No
4. Observed impact to intellectual property?	☐ Yes	☐ No
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?	☐ Yes	☐ No
Complex delivery or exfiltration techniques?	☐ Yes	☐ No
Custom, tailored, or unique tool(s) used?	☐ Yes	☐ No
Complex obfuscation techniques?	☐ Yes	☐ No
Established persistence?	☐ Yes	☐ No

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?	☐ Yes	☐ No
2. Is there national media coverage or other widely available public coverage?	☐ Yes	☐ No
3. Are foreign state adversaries tracking this incident?	☐ Yes	☐ No
4. Are foreign non-state adversaries tracking this incident?	☐ Yes	☐ No
5. Are discussions about the incident taking place in online communities?	☐ Yes	☐ 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]:

[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)
C. If the major incident involved network-based effects, not necessarily linked to mobile device access, utilize the Mobile Network-Based Effects Matrix[26]:
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?
2. 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?

[26] 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
POST-MAJOR INCIDENT UPDATE (WITHIN [7] DAYS OF RESOLUTION) (CONTINUED)
7. Describe the recovery strategy used:
8. Was the recovery strategy successful? ☐ Yes ☐ No
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]: ☐ Cyber-related Personally Identifiable Information (PII) ☐ Non-Cyber PII ☐ Both
Answer the following questions about the breach. If any of these items are answered "yes," then this breach constitutes a major incident and should be reported appropriately.
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? ☐ Yes ☐ No 2. Foreign relations of the United States? ☐ Yes ☐ No 3. Economy of the United States? ☐ Yes ☐ No 4. Public confidence of the American people? ☐ Yes ☐ No 5. Civil liberties of the American people? ☐ Yes ☐ No 6. Public health and safety of the American people? ☐ 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:

[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 Number(s)		7. Preferred Email Address of Organization (i.e., soc@organization.gov, soc@organization.com):
A. Unclassified:	B. Classified:	

8. Top-Level Organization

A. Name:	B. Type:

C. Point(s) of Contact

1. Name

First:	Middle (if applicable):	Last:	Suffix (if applicable):

2. Phone Number(s)		3. Email Address	
Unclassified:	Classified:	Unclassified:	Classified:

9. Organization Sub-Entity:	10. Critical Infrastructure Sector:

11. Identify the current level of impact on agency functions or services (Functional Impact):

12. Has someone other than an authorized user accessed or potentially accessed PII? ☐ Yes ☐ No

Alternately, has an authorized user accessed, or potentially accessed, information for an other-than-authorized purpose? ☐ Yes ☐ No

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:

Identifying Numbers

- ☐ Social Security Number: _____
- ☐ Truncated or Partial Social Security Number: _____
- ☐ Driver's License Number: _____
- ☐ License Plate Number: _____
- ☐ Drug Enforcement Administration (DEA) Registration Number: _____
- ☐ File/Case ID Number: _____
- ☐ Patient ID Number: _____
- ☐ Health Plan Beneficiary Number: _____
- ☐ Student ID Number: _____
- ☐ Federal Student Aid Number: _____
- ☐ Passport Number: _____
- ☐ Alien Registration Number: _____
- ☐ Department of Defense (DoD) ID Number: _____
- ☐ DoD Benefits Number: _____
- ☐ Employee Identification Number: _____
- ☐ Professional License Number: _____
- ☐ Taxpayer Identification Number: _____
- ☐ Business Taxpayer Identification Number (Sole Proprietor): _____
- ☐ Credit/Debit Card Number: _____
- ☐ Business Credit Card Number (Sole Proprietor): _____
- ☐ Vehicle Identification Number: _____
- ☐ Business Vehicle Identification Number (Sole Proprietor): _____
- ☐ Personal Bank Account Number: _____
- ☐ Business Bank Account Number (Sole Proprietor): _____
- ☐ Personal Device Identifiers or Serial Numbers: _____
- ☐ Business Device Identifiers or Serial Numbers (Sole Proprietor): _____
- ☐ Personal Mobile Number: _____
- ☐ Business Mobile Number (Sole Proprietor): _____

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): _____
- ☐ Gender: _____
- ☐ Race: _____
- ☐ Date of Birth (Day, Month, Year): _____
- ☐ Ethnicity: _____
- ☐ Nationality: _____
- ☐ Country of Birth: _____
- ☐ City or County of Birth: _____
- ☐ Marital Status: _____
- ☐ Citizenship: _____
- ☐ Immigration Status: _____
- ☐ Religion/Religious Preference: _____
- ☐ Home Address: _____
- ☐ Zip Code: _____
- ☐ Home Phone or Fax Number: _____
- ☐ Spouse Information: _____
- ☐ Sexual Orientation: _____
- ☐ Children Information: _____
- ☐ Group/Organization Membership: _____
- ☐ Military Service Information: _____
- ☐ Mother's Maiden Name: _____
- ☐ Business Mailing Address (Sole Proprietor): _____
- ☐ Business Phone or Fax Number (Sole Proprietor): _____
- ☐ Global Positioning System (GPS)/Location Data: _____
- ☐ Personal Email Address: _____
- ☐ Business Email Address: _____
- ☐ Employment Information: _____
- ☐ Personal Financial Information (including loan information): _____
- ☐ Business Financial Information (including loan information): _____
- ☐ Alias (i.e., username or screenname): _____
- ☐ Education Information: _____
- ☐ Resume or Curriculum Vitae: _____
- ☐ Professional/Personal References: _____

Biometrics, Distinguishing Features, and Characteristics

- ☐ Fingerprints: _____
- ☐ Palm Prints: _____
- ☐ Vascular Scans: _____
- ☐ Retina/Iris Scans: _____
- ☐ Dental Profile: _____
- ☐ Scars, Marks, Tattoos: _____
- ☐ Hair Color: _____
- ☐ Eye Color: _____
- ☐ Height: _____
- ☐ Video Recording: _____
- ☐ Photos: _____
- ☐ Voice/Audio Recording: _____
- ☐ DNA Sample or Profile: _____
- ☐ Signatures: _____
- ☐ Weight: _____

Medical and Emergency Information

- ☐ Medical/Health Information: _____
- ☐ Mental Health Information: _____
- ☐ Disability Information: _____
- ☐ Workers' Compensation Information: _____
- ☐ Patient ID Number: _____
- ☐ Emergency Contact Information: _____

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: _____
- ☐ Truncated or Partial Social Security Number: _____
- ☐ Driver's License Number: _____
- ☐ License Plate Number: _____
- ☐ Drug Enforcement Administration (DEA) Registration Number: _____
- ☐ File/Case ID Number: _____
- ☐ Patient ID Number: _____
- ☐ Health Plan Beneficiary Number: _____
- ☐ Student ID Number: _____
- ☐ Federal Student Aid Number: _____
- ☐ Passport Number: _____
- ☐ Alien Registration Number: _____
- ☐ Department of Defense (DoD) ID Number: _____
- ☐ DoD Benefits Number: _____
- ☐ Employee Identification Number: _____
- ☐ Professional License Number: _____
- ☐ Taxpayer Identification Number: _____
- ☐ Business Taxpayer Identification Number (Sole Proprietor): _____
- ☐ Credit/Debit Card Number: _____
- ☐ Business Credit Card Number (Sole Proprietor): _____
- ☐ Vehicle Identification Number: _____
- ☐ Business Vehicle Identification Number (Sole Proprietor): _____
- ☐ Personal Bank Account Number: _____
- ☐ Business Bank Account Number (Sole Proprietor): _____
- ☐ Personal Device Identifiers or Serial Numbers: _____
- ☐ Business Device Identifiers or Serial Numbers (Sole Proprietor): _____
- ☐ Personal Mobile Number: _____
- ☐ Business Mobile Number (Sole Proprietor): _____

BREACH REPORTING REQUIREMENTS

ONE-HOUR BREACH INITIAL REPORT (CONTINUED)

13. Provide known or approximate counts of all PII types that have been manipulated, destroyed, or rendered unusable:

Biographical Information

- ☐ Name (including nicknames): _____
- ☐ Gender: _____
- ☐ Race: _____
- ☐ Date of Birth (Day, Month, Year): _____
- ☐ Ethnicity: _____
- ☐ Nationality: _____
- ☐ Country of Birth: _____
- ☐ City or County of Birth: _____
- ☐ Marital Status: _____
- ☐ Citizenship: _____
- ☐ Immigration Status: _____
- ☐ Religion/Religious Preference: _____
- ☐ Home Address: _____
- ☐ Zip Code: _____
- ☐ Home Phone or Fax Number: _____
- ☐ Spouse Information: _____
- ☐ Sexual Orientation: _____
- ☐ Children Information: _____
- ☐ Group/Organization Membership: _____
- ☐ Military Service Information: _____
- ☐ Mother's Maiden Name: _____
- ☐ Business Mailing Address (Sole Proprietor): _____
- ☐ Business Phone or Fax Number (Sole Proprietor): _____
- ☐ Global Positioning System (GPS)/Location Data: _____
- ☐ Personal Email Address: _____
- ☐ Business Email Address: _____
- ☐ Employment Information: _____
- ☐ Personal Financial Information (including loan information): _____
- ☐ Business Financial Information (including loan information): _____
- ☐ Alias (i.e., username or screenname): _____
- ☐ Education Information: _____
- ☐ Resume or Curriculum Vitae: _____
- ☐ Professional/Personal References: _____

Biometrics, Distinguishing Features, and Characteristics

- ☐ Fingerprints: _____
- ☐ Palm Prints: _____
- ☐ Vascular Scans: _____
- ☐ Retina/Iris Scans: _____
- ☐ Dental Profile: _____
- ☐ Scars, Marks, Tattoos: _____
- ☐ Hair Color: _____
- ☐ Eye Color: _____
- ☐ Height: _____
- ☐ Video Recording: _____
- ☐ Photos: _____
- ☐ Voice/Audio Recording: _____
- ☐ DNA Sample or Profile: _____
- ☐ Signatures: _____
- ☐ Weight: _____

Medical and Emergency Information

- ☐ Medical/Health Information: _____
- ☐ Mental Health Information: _____
- ☐ Disability Information: _____
- ☐ Workers' Compensation Information: _____
- ☐ Patient ID Number: _____
- ☐ Emergency Contact Information: _____

BREACH REPORTING REQUIREMENTS

ONE-HOUR BREACH INITIAL 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, 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: _____

14. Was this PII observed on the Internet? ☐ Yes ☐ No If yes, provide:

Domains:	Internet Protocol (IP) Address(es):
Website(s):	Social Media Platform(s):

15. Estimate the scope of time and resources needed to recover from 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?

☐ Yes ☐ No If yes, provide:

CISA Tracking Number: _____

Organization Tracking Number: _____

20. When was the activity first detected?

20A. Describe the nature of the activity:

[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 ☐ Log Review ☐ 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) ☐ Verbal ☐ 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:

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 following events was observed.[31]

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?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

3. Government and Support Networks

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

4. Health and Public Safety

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

5. National Communications and Technology Infrastructure

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

6. Public Transportation

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

7. Public Utilities

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

B. Recognizing Impact and Effects

1. Observed impact to domestic or foreign policy?	☐ Yes	☐ No
2. Observed impact to government operations?	☐ Yes	☐ No
3. Observed impact to national or global financial systems or economy?	☐ Yes	☐ No
4. Observed impact to intellectual property?	☐ Yes	☐ No
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?	☐ Yes	☐ No
Complex delivery or exfiltration techniques?	☐ Yes	☐ No
Custom, tailored, or unique tool(s) used?	☐ Yes	☐ No
Complex obfuscation techniques?	☐ Yes	☐ No
Established persistence?	☐ Yes	☐ No

[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?	☐ Yes	☐ No
2. Is there national media coverage or other widely available public coverage?	☐ Yes	☐ No
3. Are foreign state adversaries tracking this breach?	☐ Yes	☐ No
4. Are foreign non-state adversaries tracking this breach?	☐ Yes	☐ No
5. Are discussions about the breach taking place in online communities?	☐ 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]:

[32] © 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]: ☐ Cyber-related Personally Identifiable Information (PII) ☐ Non-Cyber PII ☐ Both

Answer the following questions about the breach. If any of these items are answered "yes," then this breach constitutes a major incident and should be reported appropriately.

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[37]:

1. National security interests of the United States?	☐ Yes	☐ No
2. Foreign relations of the United States?	☐ Yes	☐ No
3. Economy of the United States?	☐ Yes	☐ No
4. Public confidence of the American people?	☐ Yes	☐ No
5. Civil liberties of the American people?	☐ Yes	☐ No
6. Public health and safety of the American people?	☐ Yes	☐ No

3. Have you previously declared this breach as a major incident? ☐ Yes ☐ No

3A. If yes, are you downgrading this from a major incident? ☐ Yes ☐ No

4. On-site or remote assistance required?

☐ Yes ☐ No If yes, identify: _____

5. Are you contracting out assistance for the reported breach? ☐ Yes ☐ No

If yes, provide name of contracted entity(ies): _____

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 required, 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))? ☐ Yes ☐ No

8C. Domains associated with the breach:

[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:
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:

[38] 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 UNTIL ALL ERADICATION ACTIVITIES COMPLETE) (CONTINUED)

8K. 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:

2. 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):

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).

9. Did this breach involve an unattributed cyber intrusion?

☐ Yes ☐ No If yes, answer whether each of the following events was observed.[39]

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?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

3. Government and Support Networks

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

4. Health and Public Safety

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

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

BREACH REPORTING REQUIREMENTS

72-HOUR BREACH UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITIES COMPLETE) (CONTINUED)

A. Understanding the Victim (Continued)

5. National Communications and Technology Infrastructure

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

6. Public Transportation

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

7. Public Utilities

Observed network intrusion or penetration?	☐ Yes	☐ No
Observed access to data storage or file systems?	☐ Yes	☐ No
Observed access to control systems?	☐ Yes	☐ No

B. Recognizing Impact and Effects

1. Observed impact to domestic or foreign policy?	☐ Yes	☐ No
2. Observed impact to government operations?	☐ Yes	☐ No
3. Observed impact to national or global financial systems or economy?	☐ Yes	☐ No
4. Observed impact to intellectual property?	☐ Yes	☐ No
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?	☐ Yes	☐ No
Complex delivery or exfiltration techniques?	☐ Yes	☐ No
Custom, tailored, or unique tool(s) used?	☐ Yes	☐ No
Complex obfuscation techniques?	☐ Yes	☐ No
Established persistence?	☐ Yes	☐ No

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?	☐ Yes	☐ No
2. Is there national media coverage or other widely available public coverage?	☐ Yes	☐ No
3. Are foreign state adversaries tracking this breach?	☐ Yes	☐ No
4. Are foreign non-state adversaries tracking this breach?	☐ Yes	☐ No
5. Are discussions about the breach taking place in online communities?	☐ Yes	☐ No

10. Using the matrices from the MITRE ATT&CK™[40] 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[41]:

[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.

[41] 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:
1. What information was needed sooner and from whom?
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?

[42] 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 UPDATE (WITHIN [7] DAYS OF RESOLUTION) (CONTINUED)
5. What precursors or indicators should be watched for in the future to detect similar breaches?
6. What additional tools or resources are needed to detect, analyze, and mitigate future breaches?
7. Describe the recovery strategy used:
8. Was the recovery strategy successful? ☐ Yes ☐ No
8A. If unsuccessful, provide details on how the strategy was revised:

EVENTS UNDER INVESTIGATION REPORTING			
72-HOUR EVENTS UNDER INVESTIGATION INITIAL REPORTING			
The below elements are strongly recommended when reporting an event under investigation for 72 hours to CISA for the first time:			
1. User Type: ☐ Impacted User ☐ Reporting on Behalf of the Impacted User			
2. Name of Reporter			
A. First:	B. Middle (if applicable):	C. Last:	D. Suffix (if applicable):
3. Phone Number(s)		4. Preferred Email Address of Organization (i.e., soc@organization.gov, soc@organization.com):	
A. Unclassified:	B. Classified:		
5. Top-Level Organization			
A. Name:		B. Type:	

EVENTS UNDER INVESTIGATION REPORTING

72-HOUR EVENTS UNDER INVESTIGATION INITIAL REPORTING (CONTINUED)

C. Point(s) of Contact

1. Name

First:	Middle (if applicable):	Last:	Suffix (if applicable):

2. Phone Number(s)		3. Email Address	
Unclassified:	Classified:	Unclassified:	Classified:

6. Organization Sub-Entity:	7. Critical Infrastructure Sector:

8. Identify the current level of impact on agency functions or services (Functional Impact):

9. Estimate the scope of time and resources needed to recover from the event (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)[44] system(s)?[45]

☐ 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
☐ 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

[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 were impacted? (Continued)

- ☐ Network Devices
  - ☐ Routers ☐ Firewalls ☐ IDS ☐ Load Balancers ☐ Other
  - ☐ Switches ☐ Proxies ☐ Intrusion Protection System (IPS) ☐ Hub
- ☐ Users

17. What network location(s) and information system(s) was the activity observed in?

17A. What network segment(s) or Virtual Local Area Network(s) was the activity observed in?

18. Describe the nature of the activity:

19. Describe how the events were detected:

20. 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:

21. Provide if available:

A. Domains associated with the event:

B. Internet protocol (IP) addresses and their relation to the event (such as attacker and victim):

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:

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 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	
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 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).	
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 Enterprise Matrix[47]:	

[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 access to a mobile device, utilize the Mobile Device Access Matrix[48]:

C. If the event involved network-based effects, not necessarily linked to mobile device access, utilize the Mobile Network-Based Effects Matrix[49]:

72-HOUR EVENTS UNDER INVESTIGATION UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITIES COMPLETE)

The below elements are strongly recommended when reporting to CISA:

1. User Type: ☐ Impacted User ☐ Reporting on Behalf of the Impacted User

2. Name of Reporter

A. First:	B. Middle (if applicable):	C. Last:	D. Suffix (if applicable):

3. Phone Number(s)		4. Preferred Email Address of Organization (i.e., soc@organization.gov, soc@organization.com):
A. Unclassified:	B. Classified:	

5. Top-Level Organization

A. Name:	B. Type:

C. Point(s) of Contact

1. Name

First:	Middle (if applicable):	Last:	Suffix (if applicable):

2. Phone Number(s)		3. Email Address	
Unclassified:	Classified:	Unclassified:	Classified:

6. Organization Sub-Entity:	7. Critical Infrastructure Sector:

8. Identify the current level of impact on agency functions or services (Functional Impact):

9. Estimate the scope of time and resources needed to recover from the event (Recoverability):

10. On-site or remote assistance required?

☐ Yes ☐ No If yes, identify: _____

[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?

☐ Yes ☐ No

13. When was the activity first detected?

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
☐ 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 ☐ Load Balancers ☐ Other
☐ Switches ☐ Proxies ☐ Intrusion Protection System (IPS) ☐ Hub

☐ Users

17. What network location(s) and information system(s) was the activity observed in?

17A. What network segment(s) or Virtual Local Area Network(s) was the activity observed in?

18. Describe the nature of the activity:

[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.

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? ☐ Yes ☐ No

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 (if applicable):	Last:	Suffix (if applicable):

B. Phone Number(s)		C. Email Address	
Unclassified:	Classified:	Unclassified:	Classified:

22. Provide if available:

A. Domains associated with the event:

B. Internet protocol (IP) addresses and their relation to the event (such as attacker and victim):

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:

23. Provide, if available and applicable:

A. Attack Vector(s) 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

EVENTS UNDER INVESTIGATION REPORTING
72-HOUR EVENTS UNDER INVESTIGATION UPDATE (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]:

[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.

[53] 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 UPDATE (CONTINUOUS UNTIL ALL ERADICATION ACTIVITIES COMPLETE) (CONTINUED)
B. If the event involved access to a mobile device, utilize the Mobile Device Access Matrix[54]:
C. If the event involved network-based effects, not necessarily linked to mobile device access, utilize the Mobile Network-Based Effects Matrix[49]:

[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.