Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination by the DHS Privacy Office to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, information collections/forms, technologies, rulemakings, programs, information sharing arrangements, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, information collection, form, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used and managed.

Please complete the attached Privacy Threshold Analysis and submit it to your component Privacy Office. After review by your component Privacy Officer the PTA is sent to the Department's Senior Director for Privacy Compliance for action. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement, or Computer Matching Agreement (CMA) – the DHS Privacy Office or component Privacy Office will send you a copy of the relevant compliance template to complete and return.

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis (PTA)

Specialized Template for
Information Collections (IC) and Forms

The Forms-PTA is a specialized template for Information Collections and Forms. This specialized PTA must accompany all Information Collections submitted as part of the Paperwork Reduction Act process (any instrument for collection (form, survey, questionnaire, etc.) from ten or more members of the public). Components may use this PTA to assess internal, component-specific forms as well.

Form Number:	**N/A**

Form Title:	Incident Reporting Form 2.0 (IRF 2.0)		
Component:	Cybersecurity and Infrastructure Security Agency (CISA)	Office:	**Cybersecurity Division (CSD)/Threat Hunting (TH)**

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	**Click here to enter text.**

OMB Control Number:	Click here to enter text.	OMB Expiration Date:	Click here to enter a date.
Collection status:	New Collection	Date of last PTA (if applicable):	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	Brian DeWyngaert		
Office:	Cybersecurity Division	Title:	Branch Chief
Phone:	202.657.1360	Email:	Brian.Dewyngaert@cisa.dhs.gov

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name:	Benjamin Thomsen		
Office:	OCIO	Title:	IT Cybersecurity Specialist

Phone:	202.254.7179	Email:	benjamin.thomsen@mail.cisa.dhs.gov

SPECIFIC IC/Forms PTA QUESTIONS

1. Purpose of the Information Collection or Form

a. Describe the purpose of the information collection or form. *Please provide a general description of the project and its purpose, including how it supports the DHS mission, in a way a non-technical person could understand (you may use information from the Supporting Statement).*
If this is an updated PTA, please specifically describe what changes or upgrades are triggering the update to this PTA.

The Cybersecurity and Infrastructure Security Agency (CISA) Office of Privacy, Access, Civil Liberties, and Transparency (PACT) is conducting a new Privacy Threshold Analysis (PTA) for the Cybersecurity Division (CSD) Threat Hunting (TH) **Incident Reporting Form 2.0 (IRF 2.0)**. IRF 2.0 will be replacing IRF 1.0. IRF 2.0 will collect more data points in a standard approach to facilitate expanded analytics. It will enable more robust reporting via end users reporting incidents and indicators as well as submitting malware artifacts associated with incidents to CISA. This information is used by DHS to conduct analyses and provide warnings of system threats and vulnerabilities, and to develop mitigation strategies as appropriate.

The CISA Incident Reporting Form provides a secure, web-enabled way to report computer security incidents to CISA. Responses provided in the form assist CISA analysts in providing timely handling of security incidents and the ability to conduct improved analysis. The IRF 2.0 can also be used for voluntary reporting or to fulfill reporting requirements form other agencies that direct reporting to CISA.

For the federal government, incident, as defined by the Federal Information Security Modernization Act of 2014 (44 USC 3552), means an occurrence that:

(A) actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Types of activity that may qualify as an incident include:

• Network intrusions that gain unauthorized access to a system or its data, including Personally Identifiable Information (PII) related incidents.

• Malicious disruption or denial of service. • The unauthorized use of a system for modifying data. • Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.
b. List the DHS (or Component) authorities to collect, store, and use this information. *If this information will be stored and used by a specific DHS component, list the component-specific authorities.*
44 U.S.C. § 3101 & 3556, 6 U.S.C. § 659(c)(1), (3), (9)

2. Describe the IC/Form	
a. Does this form collect any Personally Identifiable Information" (PII[1])?	☒ Yes ☐ No
b. From which type(s) of individuals does this form collect information? (*Check all that apply*.)	☒ Members of the public ☒ U.S. citizens or lawful permanent residents ☒ Non-U.S. Persons ☒ DHS Employees/Contractors (list Components) **All components** ☒ Other federal employees or contractors
c. Who will complete and submit this form? (*Check all that apply*.)	☒ The record subject of the form (e.g., the individual applicant). ☒ Legal Representative (preparer, attorney, etc.). ☒ Business entity. If a business entity, is the only information collected business contact information?

[1] Personally identifiable information means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

	☒ Yes ☒ No ☒ Law enforcement. ☒ DHS employee/contractor. ☒ Other individual/entity/organization **that is NOT the record subject**. *Please describe*. **Any member of the public may complete and submit the form.**
d. How do individuals complete the form? *Check all that apply.*	☐ Paper. ☐ Electronic. (ex: fillable PDF) ☒ Online web form. (available and submitted via the internet) *Provide link:* **https://myservices.cisa.gov/irf**

e. What information will DHS collect on the form? *List all individual PII data elements on the form. If the form will collect information from more than one type of individual, please break down list of data elements collected by type of individual.*

See Appendix A attached for information collected.

f. Does this form collect Social Security number (SSN) or other element that is stand-alone Sensitive Personally Identifiable Information (SPII)? *Check all that apply.* **N/A**

☐ Social Security number	☐ DHS Electronic Data Interchange Personal Identifier (EDIPI)
☐ Alien Number (A-Number)	☐ Social Media Handle/ID
☐ Tax Identification Number	☐ Known Traveler Number
☐ Visa Number	☐ Trusted Traveler Number (Global Entry, Pre-Check, etc.)
☐ Passport Number	☐ Driver's License Number
☐ Bank Account, Credit Card, or other financial account number	☐ Biometrics
☐ Other. *Please list:*	

g. List the ***specific authority*** to collect SSN or these other SPII elements.

N/A
h. How will the SSN and SPII information be used? What is the purpose of the collection?
N/A
i. Is SSN necessary to carry out the functions of this form and/or fulfill requirements of the information collection? *Note*: even if you are properly authorized to collect SSNs, you are required to use an alternative identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as truncating the SSN.
N/A

j. Are individuals provided notice at the time of collection by DHS (*Does the records subject have notice of the collection or is form filled out by third party*)?	☒ Yes. Please describe how notice is provided. **Privacy Act Statement located on the website where the form is provided.** ☐ No.

3. How will DHS store the IC/form responses?	
a. How will DHS store the original, completed IC/forms?	☐ Paper. Please describe. Click here to enter text. ☒ Electronic. Please describe the IT system that will store the data from the form. **In a CISA tracking/ticketing system, currently named Unified Ticketing System (UTS)** ☐ Scanned forms (completed forms are scanned into an electronic repository). Please describe the electronic repository. Click here to enter text.

b. If electronic, how does DHS input the responses into the IT system?	☐ Manually (data elements manually entered). Please describe. Click here to enter text. ☒ Automatically. Please describe. **After the respondent completes the online form and submits it, the information from the form is then ingested into the Unified Ticketing System. The ticket associated with the form is then routed to the appropriate service desk personnel within CISA for any required actions.**
c. How would a user search the information submitted on the forms, *i.e.*, how is the information retrieved?	☒ By a unique identifier.[2] *Please describe*. If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA. **Information may be retrieved by name, phone number, or email (if one is associated with an incident).** ☒ By a non-personal identifier. *Please describe*. **Information may be retrieved by Incident ID number, organization, type of threat indicator, or element of cyber threat intelligence (CTI).**
d. What is the records retention schedule(s)? *Include the records schedule number.*	NCPS Records Schedule (#DAA-0563-2013-0008) Data is destroyed or deleted when three years old or when no longer needed for agency business, whichever is later. Analysis and reports are destroyed or deleted when five years old or when no longer needed for agency business, whichever is later.
e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?	Automated purge.

[2] Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

f. Is any of this information shared outside of the original program/office? *If yes, describe where (other offices or DHS components or external entities) and why. What are the authorities of the receiving party?*

☒ Yes, information is shared with other DHS components or offices. Please describe.

If an incident report is submitted by a DHS component, an entity reporting pursuant to requirements promulgated by a DHS component, an entity in a sector for which a DHS component serves as the sector risk management agency, or otherwise concerns DHS, CISA may share form responses with DHS components during incident response.

☒ Yes, information is shared *external* to DHS with other federal agencies, state/local partners, international partners, or non-governmental entities. Please describe.

CISA may share any and all submitted information to external parties when relevant to the incident. For example, information could be shared when law enforcement (such as the FBI) may need to contact the submitter for additional computer security incident information. All cybersecurity information sharing is subject to the CISA Cybersecurity Information Handling Guidelines (CIHG).

To safeguard privacy, any information shared outside of the federal government will undergo a thorough anonymization process, ensuring that personal identifiers are removed. This measure ensures that data can be utilized while maintaining the confidentiality of individuals involved.

☐ No. Information on this form is not shared outside of the collecting office.

Please include <u>a copy of the referenced form and Privacy Act Statement</u> (if applicable) with this PTA upon submission.

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**Erin Alford**
Date submitted to Component Privacy Office:	**July 25, 2024**
Concurrence from other Components involved (if applicable):	N/A
Date submitted to DHS Privacy Office:	Click here to enter a date.
Have you approved a Privacy Act Statement for this form? (*Only applicable if you have received a waiver from the DHS Chief Privacy Officer to approve component Privacy Act Statements.*)	☐ Yes. Please include it with this PTA submission. ☐ No. Please describe why not. Click here to enter text.

Component Privacy Office Recommendation:
Please include recommendation below, including what existing privacy compliance documentation is available or new privacy compliance documentation is needed.

The Cybersecurity and Infrastructure Security Agency (CISA) Office of Privacy, Access, Civil Liberties, and Transparency (PACT) is conducting a new Privacy Threshold Analysis (PTA) for the Cybersecurity Division (CSD) Threat Hunting (TH) **Incident Reporting Form 2.0 (IRF 2.0)**. IRF 2.0 will be replacing IRF 1.0. IRF 2.0 will collect more data points in a standard approach to facilitate expanded analytics. It will enable more robust reporting via end users reporting incidents and indicators as well as submitting malware artifacts associated with incidents to CISA. This information is used by DHS to conduct analyses and provide warnings of system threats and vulnerabilities, and to develop mitigation strategies as appropriate.

The CISA Incident Reporting Form provides a secure, web-enabled way to report computer security incidents to CISA. Responses provided in the form assist CISA analysts in providing timely handling of security incidents and the ability to conduct improved analysis. The IRF 2.0 can also be used for voluntary reporting or to fulfill reporting requirements form other agencies that direct reporting to CISA.

For the federal government, incident, as defined by the Federal Information Security Modernization Act of 2014 (44 USC 3552), means an occurrence that:

(A) actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Types of activity that may qualify as an incident include:

- Network intrusions that gain unauthorized access to a system or its data, including Personally Identifiable Information (PII) related incidents.
- Malicious disruption or denial of service.
- The unauthorized use of a system for modifying data.
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

The CISA Office for Privacy, Access, Civil Liberties, and Transparency (PACT) recommends the Incident Reporting Form is privacy sensitive requiring PIA and SORN coverage along with a Privacy Act Statement.

CISA's Office of PACT recommends PIA coverage is provided by DHS/ALL/PIA-006 DHS General Contact Lists, which covers the collection of contact information to conduct agency operations and DHS/CISA/PIA-026 National Cybersecurity Protection System (NCPS), which covers the system used to collect cyber threat information.

CISA's Office of PACT recommends SORN coverage is provided by DHS/ALL-002 DHS Mailing and Other Lists System, which describes the collection and maintenance of records for the purpose of mailing informational literature or responses to those who request it, and for other purposes for which mailing or contact lists may be created.

Drafted Privacy Act Statement included.

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Brian Pochatila**
PCTS Workflow Number:	**0017953**
Date approved by DHS Privacy Office:	September 9, 2024
PTA Expiration Date	September 9, 2027
DHS Privacy Office Approver (if applicable):	**Riley Dean**

DESIGNATION

Privacy Sensitive IC or Form:	**Yes If "no" PTA adjudication is complete.**
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing SPII applies. ☒ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Specialized training required. ☐ Other. Click here to enter text.
Privacy Act Statement:	**e(3) statement currently accurate.** PAS submitted and approved.
System PTA:	Choose an item. Click here to enter text.
PIA:	**System covered by existing PIA** If covered by existing PIA, please list: DHS/ALL/PIA-006 DHS General Contact Lists; DHS/CISA/PIA-026 National Cybersecurity Protection System (NCPS) If a PIA update is required, please list: Click here to enter text.
SORN:	**System covered by existing SORN**

	If covered by existing SORN, please list: DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, November 25, 2008, 73 FR 71659 If a SORN update is required, please list: Click here to enter text.

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

CISA is submitting this PTA update for the Cybersecurity Division (CSD) Threat Hunting (TH) Incident Reporting Form 2.0 (IRF 2.0). IRF 2.0 will be replacing IRF 1.0. IRF 2.0 will collect more data points in a standard approach to facilitate expanded analytics. It will enable more robust reporting via end users reporting incidents and indicators as well as submitting malware artifacts associated with incidents to CISA. This information is used by DHS to conduct analyses and provide warnings of system threats and vulnerabilities, and to develop mitigation strategies as appropriate.

The CISA Incident Reporting Form provides a secure, web-enabled way to report computer security incidents to CISA. Responses provided in the form assist CISA analysts in providing timely handling of security incidents and the ability to conduct improved analysis. The IRF 2.0 can also be used for voluntary reporting or to fulfill reporting requirements form other agencies that direct reporting to CISA.

This form does not collect SSNs. It collects the number of instances that SSNs were implicated.

The DHS Privacy Office concurs that the Incident Reporting Form is privacy sensitive, requiring PIA and SORN coverage. PIA coverage is provided by DHS/ALL/PIA-006 DHS General Contact Lists, which covers the collection of contact information to conduct agency operations and DHS/CISA/PIA-026 National Cybersecurity Protection System (NCPS), which covers the system used to collect cyber threat information.

SORN coverage is provided by DHS/ALL-002 DHS Mailing and Other Lists System, which describes the collection and maintenance of records for the purpose of mailing informational literature or responses to those who request it, and for other purposes for which mailing or contact lists may be created.

APPENDIX A

Incident Reporting Form version 2.0 (IRF 2.0) Questions
This version 22 is now in use a/o 08/08/2024

Table of Contents

Legend Key

The following labels and key are provided for question marking to indicate the required and optional questions for each type of reporting entity.

[RA] = Required question for all types of reports

[RR] = Required question for reports identified as necessary to satisfy a regulatory and/or statutory requirement including Federal Information Security Modernization Act (FISMA)

[RC] = Required question based on an earlier conditional response/selection; also includes some conditional notes and logic to explain further, for example: (DESIGN NOTE: Applies to only "private sector" selection)

[FISMA Req] = Required question for reports identified as necessary to satisfy FISMA reporting requirements

[FedRAMP] = Required question for reports identified as necessary to satisfy Federal Risk and Authorization Management Program (FedRAMP) reporting requirements
[Fed Ctr] = U. S. Government Federal Contractor Only
[Op] = Optional
[Op] + [FISMA Req] = Required for FISMA reporters and optional for all other reporters.
[Op] + [RR] = Optional for all, except required for regulatory and/or statutory reporting including FISMA
[C-15] = CISA 2015 data marking option for non-Federal incident reporting. This is not a default marking, but is available for non-Federal reporters if their data meets CISA 2015 data marking criteria, e.g., cyber threat indicators (CTIs).
[CUI] = Controlled unclassified information
Design and display notes are provided to assist both the reader of the questions and the developers of the web design portal to understand both the logic flow and enhance the understanding of specific questions and terms that some readers may not be familiar with. The format for these notes is as follows:
(DISPLAY NOTE: Light blue and bolded words should be displayed to the readers.)
(DESIGN NOTE: Black and bolded words are for the developers only and should not be displayed to the readers.)
All Footnotes will be presented on the form in a method determined during the design process for the best display for the reader. These methods could be a combination of "pop-ups", on form notes, "hover-over" notes, etc.
Beginning of Incident Reporting Questions

(DISPLAY NOTE**: Global Disclaimer: Please fill out all questions in this form to the best of your knowledge at the time of submission.)**
Report Type

FOR ALL REPORTERS
[RA] What type of report do you want to submit?
Initial report
Supplemental/update report
Post-incident report[3]
Report Reason:
[RA] Why are you reporting? (select one)
Voluntarily reporting a cyber incident
Reporting to satisfy a regulatory, statutory, and/or contractual requirement
(DISPLAY NOTE: If you are a third party completing the incident report on behalf of the affected entity, please be aware that we ask for details about the affected organization first and will gather your details later in the process.)
{Conditional on selecting "2.B" above}[RR] Please identify the regulatory, statutory, and/or contractual requirement you are intending to satisfy with this report from the list below. . **(DESIGN NOTE: Multi select) (DESIGN NOTE: This question does not apply to "voluntary" identified reports) (DESIGN NOTE: All options below, unless presented with additional "report reason" choices (e.g., FISMA, FEDRAMP) are to be flagged as reporting a cyber incident".)**
(DISPLAY NOTE: To the extent that a reporting requirement provides that reporting to CISA is a means of compliance, you must indicate the specific requirement below to be considered as reporting under that requirement.)
Cybersecurity and Infrastructure Security Agency (CISA)
Federal Information Security Modernization Act of 2014 (FISMA 2014)

[3] **Post Incident "Stage" [Report]:** Report submitted at the conclusion of the incident after all recovery efforts have been completed (or at a minimum, completed efforts have been accepted by the impacted entity as sufficient). The post incident report includes information referenced in CISA's Incident Response Playbook, such as documenting lessons learned. For Federal Civilian Executive Branch reporters, this post incident report is due no later than 7 days after incident resolution.

Please select the appropriate report reason:
Cyber incident
Unauthorized release and/or loss of agency information (including personally identifiable information) unrelated to a cybersecurity incident

Federal Energy Regulatory Commission (FERC)/ North American Electric Reliability Corporation (NERC)
Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security Management Controls) and CIP-008-6 (Cyber Security – Incident Reporting and Response Planning)

Federal Risk and Authorization Management Program (FedRAMP)
Please select the appropriate report reason:
Cyber incident
Unauthorized release and/or loss of agency information (including personally identifiable information) unrelated to a cybersecurity incident

Nuclear Regulatory Commission
Cybersecurity event notifications (10 C.F.R 73.77)

Transportation Security Administration (TSA)
Security Directives or Information Circulars associated with Surface Transportation, Rail, Public Transportation and Passenger Railroad Cybersecurity (SD 1582-21-01 series, SD 1580-21-01 series, and IC 2021-01, including all amendments and successors)
Security Directives or Information Circulars associated with Pipeline Cybersecurity (SD Pipeline 2021-01 series and IC Pipeline 2022-01, including all amendments and successors)
(**DESIGN NOTE: Placeholder for aviation citations, details TBD**)
Airport Security Program (ASP)
Aircraft Operator Standard Security Program (AOSSP)
Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP)
Twelve-Five Standard Security Program (TFSSP)
Private Charter Standard Security Program (PCSSP)
Indirect Air Carrier Standard Security Program (IACSSP)
Certified Cargo Screening Standard Security Program (CCSSP)

U.S. Coast Guard (USCG)
Suspicious activity, breaches of security, or transportation security incidents (33 C.F.R 101.305 and 33 C.F.R. 6.16)

(**DESIGN NOTE: Reserved Agency details TBD if necessary**)
Reserved statute, regulation, or contractual requirement **(DESIGN NOTE: Details TBD if necessary**)
Please select the appropriate report reason:
(**DESIGN NOTE: "report reason" List**) **(DESIGN NOTE: Details TBD if necessary)**

Other (**DISPLAY NOTE: Reporters selecting this option are responsible for confirming that the listed agency and statute/regulation/contract permit reporting to CISA as a means of compliance with that agency's reporting requirements.)**
Agency [describe] **(DESIGN NOTE: Open text)**
Statute, regulation, or contract clause [describe] **(DESIGN NOTE: Open text)**
Contact Information of Reporter:
[CUI][RA] Please provide your name and contact information
[CUI]Name
First
Last
[CUI] Phone number(s)
Preferred

Alternate
[CUI] Email address(es)
Preferred
Alternate
[CUI] Social media profile (Optional)
Primary social media handle or username?
Enter the corresponding social media platform
Job title
Which time zone are you in?

[CUI][RA] Are you the primary point of contact for this incident? (Yes/No)
[RC] **(DESIGN NOTE: If Yes, set Reporter point of contact (POC)information = Primary POC)**
[CUI][RC] **(DESIGN NOTE: If No)** Please provide the primary point of contact name and contact information **(DESIGN NOTE: Set this contact as Primary POC)**
[CUI]Name
First
Last
[CUI]Phone number(s)
Preferred
Alternate
[CUI]Email address(es) of point of contact
Preferred
Alternate
[CUI] Social media profile (Optional)
Primary social media handle or username?
Enter the corresponding social media platform
Job title
Which time zone are they in?

[RA] Are we able to contact the primary point of contact for clarification or additional information not provided in this report? (Yes/No)
[RC] If yes,
What time, in your local time zone, is the best time to reach you (and/or the primary point of contact)?
What day of the week is best for us to reach out to the primary point of contact?
What is the primary point of contact's the preferred method of contact? **(DESIGN NOTE: Multi select: Phone, Email, Other [describe])** (select all that apply) Phone, Email, Other [Describe]) **(DESIGN NOTE: Open Text)**

[RA] Do you work for the affected organization [4]?
Yes
No, I am a third party and have been expressly authorized to report on the affected entity's behalf (law firm, incident response firm, etc.) **(DESIGN NOTE: Produce this "display note" upon condition the reporter is also reporting pursuant to a reporting requirement >> DISPLAY NOTE: If a third party is submitting a report on behalf of the impacted entity to satisfy another legally required reporting requirement, (1) the third-party submitter must be expressly authorized by the impacted entity to submit reports on its behalf and (2) the other reporting requirement must allow for third-party submission of reports. CISA will not verify whether third-party submission of a report fully satisfies other legal reporting requirements on behalf of an impacted entity.)**

[4] Organization: [FIPS 200, https://doi.org/10.6028/NIST.FIPS.200] An entity of any size, complexity, or positioning within an organizational structure, including federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or, as appropriate, any of their operational elements.

[CUI]Please provide the contact information for the person at the impacted entity who expressly authorized you to report on the entity's behalf.
[CUI]Name
First
Last
[CUI]Phone number(s)
Preferred
Alternate
[CUI]Email address(es) of point of contact
Preferred
Alternate
Job title
Not applicable, I am an individual, self-reporting an incident affecting me.
Impacted Entity Demographics:
(DESIGN NOTE: Section "d. Impacted Entity Demographics" does NOT apply to reporters that have identified as "I am an individual, self-reporting an incident affecting me" in previous question. Advance to Section e. Incident Notifications" for these reporters.)
[RA] What is the affected entity type?
Private sector (including U.S. Government contractors)
U.S. Federal Government agency
U.S. State, Local, Tribal, or Territorial (SLTT) entity
Foreign government entity
Civil society
Other [describe]
[RC] **(DESIGN NOTE: Applies to only "Private sector" or "Other" selection, except those private sectors that have indicated reporting for a regulatory, statutory, and/or contractual requirement intending to satisfy FISMA and or FedRAMP, then those reporters are directed to Q13 as U.S. Government contractors) Private Sector and Other (DESIGN NOTE: Display the description indicated in Q 8.F "Other" here if applicable) – Impacted Entity Demographics**
Please provide the name of the affected entity. (Please spell out any acronyms.)
Is the affected entity a subsidiary of a larger entity? (Yes/No) **(DESIGN NOTE: If Yes)** Provide the name of the larger/parent entity
Is the affected entity operating in a critical infrastructure sector[5]? (Yes/No)
{Conditional to "Voluntary" report AND "Yes" to "operating a critical infrastructure" AND "Entity Type" is not "Federal Government"} **(DESIGN NOTE: If this is flagged as a "voluntary" report and "yes" as operating a critical infrastructure and NOT a "Federal Government entity" then the following Protected Critical Infrastructure Information (PCII)conditions must be met and asked of the reporter)** You have indicated your entity operates in a critical infrastructure sector and is also submitting this report on a voluntary basis. So that your report can be evaluated for protections afforded under the Protected Critical Infrastructure Information (PCII) Program[6], do you consider the information you are sharing to meet any of the following conditions? Select "Yes" if any of the following conditions are true. (Yes/No)
Is the information, not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records, communication networks, or other information concerning:
Actual, potential, or threatened interference with, attack on, compromise or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct that violates Federal, State, local, tribal, or territorial laws, harms interstate commerce of the United States, or threatens public health or safety.
The ability of any critical infrastructure or protected system to prevent such interference, compromise, or incapacitation; including any planned or past assessment, projection, or estimate of the vulnerability of critical

[5] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[6] PCII Program - Frequently Asked Questions | CISA (https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions)

infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit.
Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.
(**DESIGN NOTE: If Yes: DISPLAY NOTE: Thank you. Your submission will be evaluated to ensure it meets the PCII program requirements. Once evaluated and requirements are validated, in order for the PCII protections to be afforded to you for this report you will need to complete and return the "Express and Consent" statement that CISA will send to you via the email contact information you provided in this form. (DESIGN NOTE: Set the "potential_PCII" variable to true.) (DISPLAY NOTE: To learn more about the benefits the PCII program affords qualified submissions please visit, https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions.))**
If you do not wish to have your submission evaluated as a PCII submission, please check this box [ ] **(DESIGN NOTE: Provide check box. When checked or activated the variable "PCII_submission_state" is set to "withdrawn", the variable "PCII_submission_withdrawal_date" is set to the current local date.)**
(**DESIGN NOTE: If No: (DISPLAY NOTE: Thank you. Your submission does not seem to meet the conditions to qualify as protected critical infrastructure information. You may now continue with the rest of the form.) (DESIGN NOTE: set the "potential_PCII" variable to false.))**
(DESIGN NOTE: If Yes) Please select the primary critical infrastructure sector that is impacted by/involved in this incident. If possible, also select the appropriate critical infrastructure critical infrastructure-subsector. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list. Primary critical infrastructure scan only be entered once.)**
Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials, and Waste
Transportation Systems
Water and Wastewater Systems
Unsure
(DESIGN NOTE: If Yes) Of the 16 listed critical infrastructure sectors, are there any additional critical infrastructure sector(s) with which your organization aligns that were also impacted by the incident? (Yes/No)
(DESIGN NOTE: If Yes, Present list of critical infrastructure again and flag as "secondary" critical infrastructure (allow multi select, but all will be flagged as "secondary")) Please select the secondary critical infrastructure sector(s) that is(are) impacted by this incident. If possible, also select the appropriate critical infrastructure critical infrastructure subsector. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list.)**

[RC] **(DESIGN NOTE: Applies to only "U.S. Federal Government agency" selection) U.S. Federal Government agency – Impacted Entity Demographics**

Please provide the Federal agency name **(DESIGN NOTE: Select from list in Appendix 5)**[7]
Please select your sub-agency below after selecting your parent agency (if applicable)**(DESIGN NOTE: Select from list in Appendix 5)**[8]**)**
We understand all incidents occurring at federal agencies impact the Government facilities critical infrastructure sector[9] and it is therefore selected as your primary critical infrastructure. However, are there any additional critical infrastructure sector(s) impacted by the incident occurring at your agency? Please select all that apply. If applicable, also select the appropriate critical infrastructure-subsector. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list. Primary critical infrastructure sector can only be entered once.) (DESIGN NOTE: Flag all Federal Gov entities as "Government facilities" for prime critical infrastructure sector, then allow for one-to-many secondary critical infrastructure sectors and sub sectors)**
Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials, and Waste
Transportation Systems
Water and Wastewater Systems
Unsure
Of the 16 listed critical infrastructure sectors, are there any additional critical infrastructure sector(s) with which your organization aligns that were also impacted by the incident? (Yes/No) **(DESIGN NOTE: If Yes, Present list of critical infrastructure again and flag as "Secondary" critical infrastructure (allow multi select, but all will be flagged as "Secondary")).** Please select the secondary critical infrastructure sector(s) that is(are) impacted by this incident. If applicable, also select the appropriate critical infrastructure-subsector. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure Sector and subsector list.)**
[RC] **(DESIGN NOTE: Applies to only "U.S. State, local, tribal, or territorial (SLTT) entity" selection) U.S. State, Local, Tribal, or Territorial (SLTT) Entity– Impacted Entity Demographics**
Please provide details about the impacted State, local, tribal, or territorial (SLTT) entity. Select from one of the below SLTT options: **(DESIGN NOTE: Single select)**
[ ] State or territory
Please provide the impacted entity's name (spell out any acronyms)
Please select your state or territory below **(DESIGN NOTE: Select from list)**[10]

[ ] Local
Please describe your local administrative division (e.g., city, district, county, township, municipality) and the U.S. state or territory your local administrative division is part of:
Please provide the impacted entity's name (spell out any acronyms)

[7] Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)
[8] Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)
[9] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[10] Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)

Please select the associated state or territory below **(DESIGN NOTE: Select from list)**[11]
[ ] Tribal
Tribal governments or communities, please indicate your tribe's name and any U.S. states and/or territories where the tribe is physically located.
Please provide the impacted entity's name
Please provide the associated U.S. states or territories for reference
Please select the associated states or territories below **(DESIGN NOTE: Select from list)**[12] **(DESIGN NOTE: Allow more than one entry as a tribe maybe physically spread across several states and regions)**
Is the impacted SLTT Entity in a critical infrastructure sector?[13] (Yes/No)
{Conditional to "voluntary" report AND "Yes" to "operating a critical infrastructure" AND "entity type" is not "Federal Government"} **(DESIGN NOTE: If this is flagged as a "voluntary" report and "Yes" as operating a critical infrastructure and NOT a "Federal Government entity" then the following PCII conditions must be met and asked of the reporter)** You have indicated your entity operates in a critical infrastructure critical infrastructure sector and is also submitting this report on a voluntary basis. So that your report can be evaluated for protections afforded under the Protected Critical Infrastructure Information (PCII) Program[14], do you consider the information you are sharing to meet any of the following conditions? Select "Yes" if any of the following conditions are true. (Yes/No)
Is the information, not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records, communication networks, or other information concerning:
Actual, potential, or threatened interference with, attack on, compromise or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct that violates Federal, State, local, tribal, territorial laws, harms interstate commerce of the United States, or threatens public health or safety.
The ability of any critical infrastructure or protected system to prevent such interference, compromise, or incapacitation; including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit.
Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.
(DESIGN NOTE: If Yes: DISPLAY NOTE: Thank you. Your submission will be evaluated to ensure it meets the PCII program requirements. Once it is evaluated and requirements are validated, you will need to complete and return the "Express and Consent" statement that CISA will send to you via the email contact information you provided in this form in order for the PCII protections to be afforded to you for this report. (DESIGN NOTE: Set the "potential_PCII" variable to true.) (DISPLAY NOTE: To learn more about the benefits the PCII program affords qualified submissions please visit, "https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions".))
If you do not wish to have your submission evaluated as a PCII submission, please check this box [ ] **(DESIGN NOTE: Provide check box. When "checked or activated" the variable "PCII_submission_state" is set to "Withdrawn", the variable "PCII_submission_withdrawl_date" is set to the current local date.)**

(DESIGN NOTE: If No: (DISPLAY NOTE: Thank you. Your submission does not seem to meet the conditions to qualify as protected critical infrastructure information. You may now continue with the rest of the form.) (DESIGN NOTE: set the "potential_PCII" variable to false.))

---

[11] Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)
[12] Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)
[13] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[14] PCII Program - Frequently Asked Questions | CISA (https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions)

(DESIGN NOTE: If Yes) Please select the primary critical infrastructure sector that is impacted by this incident. If applicable, also select the appropriate critical infrastructure-subsector. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure Sector and subsector list. Primary critical infrastructure Sector can only be entered once.)**
Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials, and Waste
Transportation Systems
Water and Wastewater Systems
(DESIGN NOTE: If Yes) Of the 16 listed critical infrastructure sectors, are there any additional critical infrastructure sector(s) with which your entity aligns that were also impacted by the incident? (Yes/No) **(DESIGN NOTE: If Yes, present list of critical infrastructures again and flag as "secondary" critical infrastructure (allow multi select, but all will be flagged as "secondary")** Please select the secondary critical infrastructure sector(s) that is(are) impacted by this incident. If applicable, also select the appropriate critical infrastructure subsector. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure Sector and Subsector list.)**

[RC] **(DESIGN NOTE: Applies to only "Foreign Government Entity" selection) Foreign Government Entity – Impacted Entity Demographics**
Please provide details about the impacted foreign entity
Please select your country below (select from list)[15]
Please provide the impacted entity's name (spell out any acronyms)
Is your entity a computer security incident response team (CSIRT)? (Yes/No)
(DESIGN NOTE: If Yes, show question) Please enter the name of the CSIRT **(DESIGN NOTE: Open text)**
Is the impacted entity in a critical infrastructure sector[16] (based on U.S. designation) (Yes/No)
(DESIGN NOTE: If Yes) Please select the primary critical infrastructure sector that is impacted by this incident. If applicable, also select the appropriate critical infrastructure-subsector. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list. Primary critical infrastructure sector can only be entered once.)**
Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture

[15] Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)
[16] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials, and Waste
Transportation Systems
Water and Wastewater Systems
Unsure
(DESIGN NOTE: If Yes) Of the 16 listed critical infrastructure sectors, are there any additional critical infrastructure sector(s) with which your entity aligns that were also impacted by the incident? (Yes/No/Unsure)
(DESIGN NOTE: If Yes, present list of critical infrastructures again and flag as "secondary" critical infrastructure (allow multi select, but all will be flagged as "secondary") Please select the secondary critical infrastructure sector(s) impacted by this incident. If applicable, also select the appropriate critical infrastructure-subsector. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list.)**
[RC] **(DESIGN NOTE: applies to only "FISMA and/or FEDRAMP" regulatory selection plus "private sector" organization type "aka entity is a U.S. Federal Government contractor") U.S. Federal Government Contractor – Impacted Entity Demographics**
Please provide the impacted Federal agency you are supporting **(DESIGN NOTE: Select from list in Appendix 5)**[17]
Please select the sub-agency below, if applicable) **(DESIGN NOTE: Select from list in Appendix 5)**[18]
We understand that all incidents occurring at federal agencies impact the government facilities critical infrastructure sector and have therefore selected it as your primary critical infrastructure sector. Are there any additional critical infrastructure sector(s) impacted by the incident occurring at your agency? Please select all that apply. If applicable, also select the appropriate critical infrastructure-subsector.
(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list. Primary critical infrastructure sector can only be entered once.) (DESIGN NOTE: Flag all Federal Gov entities as "government facilities" as their prime critical infrastructure sector, then allow for one-to-many secondary critical infrastructure sectors and sub sectors.)
Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials, and Waste
Transportation Systems
Water and Wastewater Systems
Unsure
Of the 16 listed critical infrastructure sectors, are there any additional critical infrastructure sector(s) with which your organization aligns that were also impacted by the incident? (Yes/No/Unsure) **(DESIGN NOTE: If Yes, Present list of critical infrastructures again and flag as "secondary" critical infrastructure (allow multi select, but all will be flagged as "secondary")** Please select the secondary critical infrastructure sector(s) impacted by this

[17] Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)
[18] Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)

incident. If applicable, also select the appropriate critical infrastructure-subsector. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list.)**
[Fed Ctr] Please enter the contract number(s), clearance level (contract and facility), and prime contractor information and points of contact that correspond to the primary contract impacted by or involved in this incident. **(DESIGN NOTE: Allow one to many entries) (DESIGN NOTE: Allow "button" to add to the contract list if necessary and repeat the following as necessary for each contract entered)**
Contract number(s)
Contract or other agreement clearance level
Unclassified
Confidential
Secret
Top Secret
Not Applicable
[Fed Ctr] Has the impacted entity been granted a facility security clearance? (Yes/No)
(DESIGN NOTE: If Yes) [Fed Ctr] What is the facility clearance level (FCL) of the impacted entity?
Unclassified
Confidential
Secret
Top Secret (may or may not include Sensitive Compartmented Information)
Not applicable
Are you the prime contractor under this contract? (Yes/No)
(DESIGN NOTE: If No) Please provide the prime contractor point of contact
Name
First
Last
Phone number(s)
Email address(es)
Position/title
Address
Street name and number
Postal code
City
State
Country
Time zone
[Fed Ctr] Please provide your US government contracting point(s) of contact **(DISPLAY NOTE: Examples of possible US government contracting points of contact are typically the Contracting Officer (CO), Contracting Officer Representative (COR), US Government Administrative Contracting Officer (ACO)**[19] **and US Government Program Manager (PM).) (DESIGN NOTE: Allow for more than one entry)**
Name
First
Last
Phone number(s)
Email address(es)
Position/title[20] (e.g., CO, COR, ACO, PM) **(DESIGN NOTE: Provide "dropdown list" to select from example list, allow "OTHER" with a fill-in description)**

[19] 48 CFR § 842.271 - Administrative Contracting Officer's role in contract administration and delegated functions. | Electronic Code of Federal Regulations (e-CFR) | US Law | LII / Legal Information Institute (cornell.edu
[20] DESIGN NOTE: for each Position selected provide "DISPLAY NOTE" as appropriate:
CO – person who has authority over the contract and ability to direct contractor activities; COR - POCs could be a federal employee who has authority and ability to direct contractor activities; ACO - Unless you are supporting the

Address
Street name and number
Postal code
City
State
Country
Time zone

[RC] **(DESIGN Note: Applies to only "civil society" selection) Civil Society – Impacted Entity Demographics**
Please provide details about the impacted civil society entity
Please describe your organization's sector within civil society (e.g., academia, faith-based, think tank, media, advocacy, political party, labor union) **(DESIGN NOTE: Open text)**
Please enter the civil society entity's name (spell out any acronyms)
Are there any critical infrastructure (critical infrastructure) sector(s)[21] directly impacted by the incident that occurred/is occurring at your organization? (Yes/No)
{Conditional to "voluntary" report AND "Yes" to "operating a critical infrastructure" AND "entity type" is not "Federal Government"} **(DESIGN NOTE: If this is flagged as a "voluntary" report and "Yes" as operating a critical infrastructure and NOT a "Federal Government entity" then the following PCII conditions must be met and asked of the reporter)** You have indicated your entity directly impacts a critical infrastructure sector and is also submitting this report on a voluntary basis. So that your report can be evaluated for protections afforded under the Protected Critical Infrastructure Information (PCII) Program[22], do you consider the information you are sharing to meet any of the following conditions? Select "Yes" if any of the following conditions are true. (Yes/No)
Is the information, not customarily in the public domain and related to the security of critical infrastructure or protected systems, including documents, records, communication networks, or other information concerning:
Actual, potential, or threatened interference with, attack on, compromise or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct that violates Federal, State, local, tribal, territorial laws, harms interstate commerce of the United States, or threatens public health or safety.
The ability of any critical infrastructure or protected system to prevent such interference, compromise, or incapacitation; including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit.
Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.
(DESIGN NOTE: If Yes: DISPLAY NOTE: Thank you. Your submission will be evaluated to ensure it meets the PCII program requirements. Once it is evaluated and requirements are validated, you will need to complete and return the "Express and Consent" statement that CISA will send to you via the email contact information you provided in this form in order for the PCII protections to be afforded to you for this report. (DESIGN NOTE: Set the "potential_PCII" variable to true.) (DISPLAY NOTE: To learn more about the benefits the PCII program affords qualified submissions please visit, "https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions".))
If you do not wish to have your submission evaluated as a PCII submission, please check this box [ ] **(DESIGN NOTE: Provide check box. When "checked or activated" the variable "PCII_submission_state" is set to "Withdrawn", the variable "PCII_submission_withdrawl_date" is set to the current local date.)**

VA or DOD it is unlikely that you have an ACO; PM – person overseeing the technical effort and has the authority to direct contractor activities.)

[21] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[22] PCII Program - Frequently Asked Questions | CISA (https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/pcii-program-frequently-asked-questions)

(DESIGN NOTE: If No: (DISPLAY NOTE: Thank you. Your submission does not seem to qualify as protected critical infrastructure information. You may now continue with the rest of the form.) (DESIGN NOTE: set the "potential_PCII" variable to false.))

(DESIGN NOTE: If Yes) Please select all critical infrastructure sectors impacted by this incident. If applicable, also select the appropriate critical infrastructure-subsector. **(DESIGN NOTE: Multi select) (DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list.)**
Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials, and Waste
Transportation Systems
Water and Wastewater Systems
Unsure
[Op] + [FISMA Req] What is the primary website of the impacted entity?
[Op] + [FISMA Req] Please enter the impacted entity's internal tracking number(s) related to this incident, (e.g. case number), if applicable. **(DESIGN NOTE: if "N/A" is selected, internal tracking number can be blank)**
Not applicable **(DESIGN NOTE: Radio button)**
Internal tracking number(s) **(DESIGN NOTE: Text box)**
[Op] + [RR] If applicable, provide the primary location and/or facility address where this incident or event occurred. (If applicable, you can also add secondary locations).
. **(DESIGN NOTE: Allow one to many entries. Flag all but first entry as "secondary" addresses of the impacted entity.)**
Not applicable **(DESIGN NOTE: Radio button - Allow to bypass "address info" if not applicable is selected)**
Name of primary (secondary if applicable) location (e.g., building name, pipeline designation, data center, shipping port, airport, telecom site, etc.) if applicable**. (DESIGN NOTE: Open text and allow "not applicable" as selection option for name. Also, either address info should be entered, or the latitude and longitude of the location should be entered. both could be allowed, but at least one location designation should be required)**
Street name and number
City
State
Postal code
Country[23]
If the incident occurred in a location without a known address, please provide the coordinates (latitude and longitude) to the best of your ability for the location of the incident. **(DISPLAY NOTE: Many critical infrastructure sector facilities, such as cellular towers in the communications sector or offshore oil platforms in the oil and natural gas (ONG) subsector, do not have street addresses. Understanding the geographic location can help CISA identify a potential targeting effort by an adversary.) (DESIGN NOTE: Include an**

[23] Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)

option to enter latitude and longitude with guidance on how to use Google Maps to quickly findl the coordinates.)
Not applicable **(DESIGN NOTE: Radio button - Allow to bypass "latitude and longitude info" if not applicable is selected)**
Latitude
Longitude
Has the incident occurred on or involved a movable entity (e.g., ship, aircraft, train)? (Yes/No)
(DESIGN NOTE: If Yes) Please describe the entity that was involved in this incident. **(DESIGN NOTE: Open text)**
[Op] + [RR] Please provide the following information about the impacted organization. (Answer for the impacted entity and not the parent entity.)

A. Do you know if the impacted entity that owns and/or operates the facility(ies) where the incident occurred has any unique government or business identifiers (e.g. North American Industrial Classification System (NAICS), General Services Administration (GSA)-issued Unique Entity Identifier (UEI))? (Yes/No/Unknown)
   i. [RC] **(DESIGN NOTE: If yes)** Please select from the identifier(s) below and provide their corresponding numbers: **(DESIGN NOTE: Multi select). (DESIGN NOTE: Provide reporters ability to use "Identifier" responses for a "look-up" to help pre-populate the following questions and ask to validate/edit)**

Type of Identifier(s)
North American Industrial Classification System (NAICS) identifier(s)
Identifier number(s) **(DESIGN NOTE: Repeated for each identifier selected)**
General Services Administration (GSA)-issued Unique Entity Identifier (UEI)
Environmental Protection Agency FacID
What are the Commercial and Government Entity (CAGE) Code(s) for the facility location(s) of the impacted system(s)? **(DESIGN NOTE: Allow for the location(s) previously entered at "Incident location" to be presented and allow the reporter to select from them. If not available to present, allow the reporter to add another address here.)**
Provide the address of the facility or facilities associated with the CAGE codes. **(DISPLAY NOTE: CAGE codes are assigned to suppliers to various government or defense agencies, as well as to government agencies themselves and various organizations. CAGE codes provide a standardized method of identifying a given facility at a specific location.)**
Street name and number
Building number (if applicable)
Suite number (if applicable)
City
State
Postal code
Country[24]
Other [please provide the type of identifier]

[24] Use CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com)

[RC] **(DESIGN Note: applies only to "Third Party" selection in "red box")**

[RA] Do you work for the affected organization [2]?
A. Yes
B. No, I am a third party and have been expressly authorized to report on the affected entity's behalf (Law firm, incident response firm, etc.) (DESIGN NOTE:|
C. Not Applicable, I am an individual, self-reporting an incident affecting me.

You indicated you are a third party authorized to report on behalf of the affected entity. What is the name of your organization? (Please spell out any acronyms)
Is your organization a subsidiary of a larger organization? (Yes/No)
(DESIGN NOTE: If Yes) Provide the name of the larger/parent organization.
What is the preferred email address of the parent organization (e.g., soc@organization.gov, soc@organization.com)?
[Op] What is the primary website of the parent organization?
[Op] Please enter the impacted entity's internal tracking number(s) related to this incident, (e.g., case number), if relevant. **(DESIGN NOTE: If "Not applicable" selected, internal tracking number can be blank)**
Not applicable **(DESIGN NOTE: Radio button)**
Internal tracking number(s)
Please provide the following information about your organization. (Please answer for your organization and not any parent organization.)
What is the preferred email address of your organization?
What is the primary website of your organization?
[Op] Please enter the impacted entity's internal tracking number(s) related to this incident, (e.g.case number), if relevant. **(DESIGN NOTE: If "not applicable" is selected, internal tracking number can be blank)**
Not applicable **(DESIGN NOTE: Radio button)**
Internal tracking number(s)

Incident Notifications

[RA] Have you already notified or reported this incident to an entity other than CISA or do you plan to notify or report this incident to an entity other than CISA? (Yes/No) **(DISPLAY NOTE: CISA will not use information reported to fulfill any additional legally required reporting obligations on your or your organization's behalf. Reporting to CISA only satisfies legally required reporting requirements to the extent that the reporting requirement explicitly provides that reporting to or through CISA is a means of compliance.) (DESIGN NOTE: Report times in Universal Time Coordinated (UTC) or local time with UTC offset. (Multi select and should be repeatable to document more than one of same point of contact type. Consider allowing reporter to enter in notification details in an update/supplemental report to speed initial reporting))**
[CUI]{Conditional} [FISMA Req] **(DESIGN NOTE: If Yes)** Please list the entities you will, or did, report to. Information owners (including information managed by the affected/reporting entity (e.g., cloud provider), and information owned by the affected/reporting entity's customer/client agency (e.g., customer owned information managed by a contracted 3rd party) **(DESIGN NOTE: Repeat the following for each notification entity selected, can also be more than one entry per category, e.g., law enforcement can be local and federal notifications)**
[CUI]Point of contact name
First
Last
Already notified: Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -<UTC offset>)
Case/incident/report number provided (if applicable)
Inspector general
Legal counsel
Law enforcement
Regulatory agency
Privacy officials
Security staff
System owners
Other

[CUI] {Conditional} [FISMA Req] **(DESIGN NOTE: If Yes)** Have you already, or are you planning to report this incident to any federal government agency other than CISA?
[If Yes] Which agency? **(DESIGN NOTE: Select from agency list in Appendix 5)**
[CUI]Point of contact name
First
Last
Already notified: Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -<UTC offset>)
Case/incident/report number provided (if applicable)
(DESIGN NOTE: All other reporters not FISMA) [CUI]{Conditional} [Op] **(DESIGN NOTE: If Yes)** Please list the entities you will, or did, report to. **(DISPLAY NOTE: This information may be helpful for CISA to understand if there are other entities that CISA may need to collaborate with or allow for special considerations during any incident response efforts.)**
Information owners (examples include information managed by affected/reporting entity (e.g., cloud provider) but owned by affected/reporting entity's customer/client) **(DESIGN NOTE: Repeat the following for each notification entity selected, can also be more than one entry per category, e.g., law enforcement can be local and federal notifications.)**
[CUI]Point of contact name
First
Last
Already notified: Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -<UTC offset>)
Case/incident/report number provided (if applicable)
Law enforcement
Regulatory agency
Other federal agencies
If selected, which agency? **(DESIGN NOTE: Select from agency list in Appendix 5)**
Other

Incident: Severity Assessments

27. Confidentiality, Integrity, Availability (CIA) Assessment[25]

[RA] (**DESIGN NOTE: Logic of all "None" applicable to FISMA reporters – Only. This is an Event-Incident FLAG for FISMA reporters only. If Q21 A-C are answered "no", that terminates the rest of the Incident Questions for a FISMA reporter, and the FISMA reporter is directed towards filling out "Event Reporting" only.)** At this time, is this incident known to either imminently[26] or actually jeopardize, without lawful authority, any of the following relating to either information or an information system? (select all that apply) **(DESIGN NOTE: For non-FISMA reports, there must be at least one selection from CIA below that is either "imminently" or "actually" selected, the other two options can be "unsure" or "none" if applicable, otherwise if all are "unsure" or "none", then the event does NOT meet threshold for an "incident". Consider, if all non-FISMA reports select "unsure/None" for all three CIA questions, then DISPLAY NOTE: You have not indicated an impact on at least one of the three areas of confidentiality, integrity, or availability per the definition of an incident.)**

[25] The concepts of confidentiality, integrity, and availability (CIA), often referred to as the "C-I-A triad," represent the three pillars of information security. See, e.g., NIST, NIST Special Publication 1800-25 Vol. A, Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events, at 1 (Dec. 2020), available at https://csrc.nist.gov/pubs/sp/1800/25/final

[26] Imminently: [a. Imminent] "ready to take place; happening soon" or " something bad or dangerous seen as menacingly near." [b. Imminent danger] "[Such an appearance of threatened and impending injury [could change to harm to an entity's information or information systems] as would put a reasonable and prudent [person] to his instant defense." Specifically surrounding networks and data imminently implies there is reasonable suspicion a threat is going to target my entity's information or information systems. [derived from a. Webster's Dictionary and b. Black's Law Dictionary {respectively}]

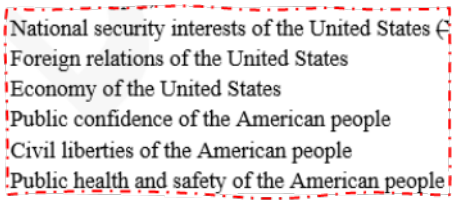
Confidentiality[27] [] imminently; [] actually; [] unsure []/none **(DESIGN NOTE: Have radio button for all)**
Integrity,[28] [] imminently; [] actually; [] unsure/none **(DESIGN NOTE: Have radio button for all)**
Availability[29] [] imminently; [] actually; [] unsure/none **(DESIGN NOTE: Have radio button for all)**
[RA] At this time, does this incident constitute an imminent or actual violation of law, security policies, security procedures, or acceptable use policies? (Yes/No) **(DESIGN NOTE: If Yes)** Please make selection(s) below
Violation of law [] imminently; [] actually; [] unsure/none **(DESIGN NOTE: Single select have radio button for all.)**
Security policies and/or procedures [] imminently; [] actually; [] unsure/none **(DESIGN NOTE: Single select have radio button for all.)**
Acceptable use policies [] imminently; [] actually; [] unsure/none **(DESIGN NOTE: Single select have radio button for all.)**

28.
29. Incident: High-Level Impacts
30. Public Impacts

National US Impacts
(DESIGN NOTE: Major Incident Flag Questions. Any "Yes" answer here is used to determine if the reporter is reporting a major incident as defined by FISMA in the next question by adding in "Demonstrable Harm" for those that selected "Yes" here.)
[Op] + [FISMA Req] To the best of your knowledge, does the incident likely impact any of the following? (Select all that apply)

A. National security interests of the United States
B. Foreign relations of the United States
C. Economy of the United States
D. Public confidence of the American people
E. Civil liberties of the American people
F. Public health and safety of the American people

(DESIGN NOTE: Major Incident - FLAG Questions: For "Q24" question, users should see all options from "Q 23 that they selected.**, "the incident is likely to result in any impact to**" above for which the answer was selected. This is a distinction for FISMA reports only) (DISPLAY NOTE: Any impacts selected with a "demonstrable harm" severity, will indicate that the incident is considered a major incident" under FISMA reporting.)
[Op] + [FISMA Req] At the time of this report, of the likely impacts of this incident selected above, are any of them likely to result in **demonstrable harm** to the United States? **(DISPLAY NOTE: Select those that are likely to result in demonstrable harm.) (DESIGN NOTE: Allow display of selected from list of selected choices here in "red box":**



from Q 23 with a "check box" to also flag for "demonstrable harm".)

Regional Impacts (Local to Global)
(DESIGN NOTE: NCISS Variable = Regional Impact (NEW, not currently mapped in algorithm from reporter's response)

[27] "Confidentiality" refers to "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." [e.g., threat actor has access to your information or an information system, without consent.]
[28] "Integrity" refers to "guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity." [e.g., a threat actor has modified or deleted your information, without your consent.]
[29] "Availability" refers to "ensuring timely and reliable access to and use of information." [e.g., a threat actor has impeded you from accessing or operating the information system or information in the way you intended (DDOS)]

[Op] + [RR] To the best of your knowledge, describe the extent of the incident's impact on the population/geographic region
Internal/site-specific (Impacts are felt by the impacted entity or a particular facility or site, but not externally)
Local (Impact is limited to entities or customers in the immediate area (e.g., town, city) external to the core business of the affected entity)
State/territory-wide
Regional
Multi-regional
National
Multi-national
Global
Unknown

Breach[30] Severity Impacts
[Op] + [FISMA Req] At this time, has the incident resulted in any confirmed unauthorized access to personally identifiable information? (Yes/No) **(DESIGN NOTE: If Yes, flag as Breach Incident and include Incident Stage (A): Breach Details. Show follow-on short questions "access due" and "accessed by" only if "Yes".)**
Was the access due to (select all that apply):
Loss of control
Compromise
Unauthorized disclosure
Unauthorized acquisition
Was the information accessed by (select all that apply):
A person other than an authorized user
An authorized user who accessed the record(s) for an other-than-authorized purpose

{Conditional}[Op] + [FISMA Req] **(DESIGN NOTE: Do not ask this question if the "Confirmed Unauthorized Access" question yields a positive selection response. Only ask if previous response to "confirmed" = "No")** At this time, has the incident resulted in any potential unauthorized access to personally identifiable information? (Yes/No) **(DESIGN NOTE: If Yes, flag as Breach Incident and include Incident Stage (A): Breach Details. Show follow-on short questions "access due" and "accessed by" only if "Yes".)**
Was the potential unauthorized access due to: (select all that apply)
Loss of control
Compromise
Unauthorized disclosure
Unauthorized acquisition
Was the information potentially accessed by (select all that apply)
A person other than an authorized user
An authorized user who accessed the information for an other-than-authorized purpose
(DESIGN NOTE: Following responses for Q26 and Q27, if breach severity "confirmed or potential unauthorized access" = Yes, DISPLAY on "POP UP SCREEN", display note to reporter: "You have indicated you have had an actual or potential breach and impacts to PII. You will be given an opportunity to provide more details on the types of PII impacted later in this report.")
Major Incident Severity Determination (FISMA Only)
[FISMA Req] At the time of this report, did any of the following occur involving personally identifiable information? **(DESIGN NOTE: Major Incident - FLAG Question: Only appears if Breach Severity "Confirmed or Potential Unauthorized Access" = Yes. If any "100,000" field is answered yes below, flag as**

[30] Breach: "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other-than-authorized purpose." per OMB M-17-12

major incident. (DESIGN NOTE: a FISMA major Incident = a significant cyber incident) (DESIGN NOTE: multi select) (DISPLAY NOTE: Select all that apply)
[ ] Unauthorized modification
(DESIGN NOTE: If selected display following:)
Was this a [ ] potential or [ ] actual occurrence?
Did this occurrence or potential occurrence involve the PII of 100,000 or more people? (Y/N)
[ ]Unauthorized deletion
(DESIGN NOTE: If selected display following:)
Was this a [ ] potential or [ ] actual occurrence?
Did this occurrence or potential occurrence involve the PII of 100,000 or more people? (Y/N)
[ ]Unauthorized exfiltration
(DESIGN NOTE: If selected display following:)
Was this a [ ] potential or [ ] actual occurrence?
Did this occurrence or potential occurrence involve the PII of 100,000 or more people? (Y/N)
[ ]Unauthorized access
(DESIGN NOTE: If selected display following:)
Was this a [ ] potential or [ ] actual occurrence?
Did this occurrence or potential occurrence involve the PII of 100,000 or more people? (Y/N)
[FISMA Req] At the time of this report, has your answer to any item within the preceding "major incident severity" questions changed since a previous report? (Yes/No) **(DESIGN NOTE: Only show if "supplemental/update" or "post-incident" report is selected)**
(DESIGN NOTE: If Yes) Did this change cause the report to (Select one response)
[ ]Upgrade to a major incident?
Please provide additional context for the change
[ ]Downgrade from a major incident?
Please provide additional context for the change
[ ]No change in major incident determination (the incident was either previously not determined to be a major incident and remains as such, or was previously determined to be a major incident and remains as such)
Please provide additional context
[FISMA Req] **(DESIGN NOTE: Only asked of FISMA reporters if the incident has been indicated as a "Major Incident" per thresholds in questions 24 and/or 28.)** Has this incident been reported to Congress? (Yes/No)
Public Health and Safety Impacts
[Op] + [RR] To the best of your knowledge, what is the current impact of this incident on public health? **(DISPLAY NOTE: Public health impacts are defined as "impacts on an affected population measured based on new and increased death, disease, injury, and disability." Impacts to access to medical care are considered public safety impacts, which are addressed in a later question.)**
(DESIGN NOTE: NCISS Variable = Public Health Impact (NEW, not currently mapped in algorithm from reporter's response)
No impact – Incident has no impact on public health
Low impact – Incident has resulted in one or more minor injuries and/or temporary disabilities that have not required emergency response (e.g., minor symptoms prompting self-care)
Moderate impact – Incident has resulted in one or more moderate injuries and/or lasting disabilities that have required emergency response and/or risk (e.g., easily treated symptoms or hospital diagnostic visits)
High impact – Incident has resulted in one or more serious injuries that have required emergency response and/or permanent disabilities
Critical impact – Incident has resulted in one or more deaths
Unknown impact – Reporter does not have information required to assess the impact of the incident on public health
[Op] + [RR] To the best of your knowledge, what is the current impact of this incident on public safety **(DISPLAY NOTE: Public safety impacts are defined as "Impact measured based on an affected population's ability to obtain shelter (e.g., temporary housing, temperature regulation), healthcare (e.g., emergency response services, open hospital beds), and lifeline resources (e.g., clean air and water, nutrition, hydration,**

communication – phone and internet service) and to maintain physical safety (e.g., data breaches that threaten individual safety).")
(DESIGN NOTE: NCISS Variable = Public Safety Impact (NEW, not currently mapped in algorithm from reporter's response))
No impact – Incident has no impact on public safety
Low impact – Incident has minimal impact on public safety (e.g., limited, short term disruption of essential services and/or lifeline resources – phone and internet service, electricity, water)
Moderate impact – Incident has more extensive impact on public safety (e.g., longer-term disruption of lifeline resources such as phone, internet, electricity, and water; healthcare and shelter impacts/disruptions from loss of electricity for extended period)
High impact – Incident has severe impact on public safety (e.g., evacuation and temporary housing of displaced communities; immediate threats to physical safety of the public; extended disruption of essential services; stress on healthcare resources; water and air contamination)
Critical impact – Incident has catastrophic impact on public safety (e.g., long-term environmental contamination; cessation of essential services such as law enforcement and healthcare; societal instability)
Unknown impact – Reporter does not have the information required to assess the impact of the incident on public safety
Indirect Impacts
[Op] + [RR] To the best of your knowledge, were/are there any indirect (or secondary) impacts to other critical infrastructure sector(s)[31]? (Yes/No)
(DESIGN NOTE: If Yes) Please select the appropriate critical infrastructure sector and the appropriate critical infrastructure subsector(s) (if applicable) that were indirectly impacted, and indicate what type of impact (functional, informational, economic and/or physical). **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list.)**
(DESIGN NOTE: Multi select) (DISPLAY NOTE: Indirect impact is defined as "an effect that is not a direct consequence of an incident, but is caused by a direct consequence, subsequent cascading effects, and/or related decisions. For example, if an electric power plant is the victim of a malicious cyber incident, directly impacting the provision of energy sector services (in this case, electricity), other local or regional sectors that are dependent on that electricity – e.g., commercial facilities and critical manufacturing – may experience indirect impacts.")
(DESIGN NOTE: NCISS Variable = Cross Sector [Indirect] Impact (NEW, not currently mapped in algorithm from reporter's response)
Chemical **(DESIGN NOTE: Multi select include any subsector lists from Appendix 4 as necessary and repeat the four "impact" selections per critical infrastructure-cross sector and/or subsector instance selected)**
Type(s) of Impact: **(DESIGN NOTE: Multi select) (DISPLAY NOTE: Select all that apply)**
Functional impact[32]
Informational impact[33]
Economic impact[34]

[31] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[32] **Functional impact:** A measure of the actual, ongoing impact to the organization. In many cases (e.g., scans and probes or a successfully defended attack), little or no impact may be experienced due to the incident (CISA National Incident Cyber Scoring System). CISA National Cyber Incident Scoring System (NCISS) | CISA

[33] **Informational Impact**: In addition to functional impact, incidents may also affect the confidentiality, integrity and availability of the information stored or processed by various systems. The information impact category is used to describe the type of information lost, compromised, or corrupted. (CISA National Incident Cyber Scoring System). CISA National Cyber Incident Scoring System (NCISS) | CISA

[34] **Economic Impact**: Any costs or losses experienced due to an incident, including the general categories listed in this form in question #38A-G. These categories are more specifically defined in the CISA report: "Cost of Cyber Incident;" see Table 44 in Appendix C, https://www.cisa.gov/sites/default/files/2023-01/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf

Physical impact [35]
Subsector list (if available) here: **(DESIGN NOTE: Multi select) (DISPLAY NOTE: Select all that apply)**
Type(s) of Impact:
Functional impact
Informational impact
Economic impact
Physical impact
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Materials, and Waste
Transportation Systems
Water and Wastewater Systems
Unknown
(DESIGN NOTE: **NCISS Variable = Part of Cross-Sector + Informational Impact (NEW, not currently mapped in algorithm from reporter's response. Needs to be added)**

[Op] + [RR] To the best of your knowledge, what is the current functional, informational, economic, and/or physical impact to other third parties that are not entities in a critical infrastructure sector? **(DESIGN NOTE: Multi select)**
Functional impact
Not applicable, there is no possibility of indirect functional impact to entities not in a critical infrastructure sector
No impact at this time
Minimal impact
Significant impact
Unrecoverable impact
Unknown
Informational impact
Not applicable, there is no possibility of indirect informational impact to entities not in a critical infrastructure sector
No impact at this time
Minimal impact
Significant impact
Unrecoverable impact
Unknown
Economic impact
Not applicable, there is no possibility of indirect economic impact to entities not in a critical infrastructure sector
No impact at this time
Minimal impact
Significant impact
Unrecoverable impact
Unknown

[35] **Physical Impact**: The resultant of an incident that has caused intentional or accidental damage to a physical system/facility/surrounding environment, that disrupts, incapacitates, or destroys reliable operations of critical infrastructure, including personnel therein.

Physical impact
Not applicable, there is no possibility of indirect physical impact to entities not in a critical infrastructure sector
No impact at this time
Minimal impact
Significant impact
Unrecoverable impact
Unknown

31. Impacts Internal to the Entity

Functional Impacts to Entity

[Op] + [RR] To the best of your knowledge, what is the current functional impact[36] of this incident?
(DESIGN NOTE: NCISS Variable = Functional Impact)
No impact **(DISPLAY NOTE: Incident has no impact.)**
No impact to services **(DISPLAY NOTE: Incident has no impact on any business or industrial control systems (ICS) services or on delivery to entity customers.)**
Minimal impact to non-critical services **(DISPLAY NOTE: Some small level of impact to non-critical systems and services.)**
Minimal impact to critical services[37] **(DISPLAY NOTE: Minimal impact to a critical system or service (e.g., email, active directory).)**
Significant impact to non-critical services **(DISPLAY NOTE: A non-critical service or system has a significant impact.)**
Significant impact to critical services **(DISPLAY NOTE: A non-critical system's access is denied, or system's functionality is destroyed.)**
Denial of non-critical services **(DISPLAY NOTE: A critical system has a significant impact (e.g., local administrative account compromise).)**
Denial of critical services/loss of control **(DISPLAY NOTE: A critical system has been rendered unavailable.)**
Unknown

Informational Impacts to Entity

(DESIGN NOTE: NCISS Variable = Part of Informational Impact (NEW, not currently mapped in algorithm from reporter's response. Needs to be added.) (Recommend this question become the primary info impact question for NCISS use and the following information impact details question later be used to gather more specifics, but not be used for "scoring.")
[Op] + [RR] To the best of your knowledge, what is the current informational impact[38] of this incident?
No impact
Minimal impact
Significant impact
Unrecoverable impact
Unknown

Physical Impacts to Entity

(DESIGN NOTE: NCISS Variable = Physical Impact (NEW, not currently mapped in algorithm from reporter's response.)

---

[36] **Functional impact** is a measure of the actual, ongoing impact to the organization. In many cases (e.g., scans and probes or a successfully defended attack), little or no impact may be experienced due to the incident (CISA National Incident Cyber Scoring System). *CISA National Cyber Incident Scoring System (NCISS) | CISA*

[37] **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. *Derived from "critical asset" page 135-136 and critically page 139 of https://www.dhs.gov/publication/dhs-lexicon*

[38] **Informational Impact**: In addition to functional impact, incidents may also affect the confidentiality, integrity and availability of the information stored or processed by various systems. The information impact category is used to describe the type of information lost, compromised, or corrupted. (CISA National Incident Cyber Scoring System). *CISA National Cyber Incident Scoring System (NCISS) | CISA*

[Op] + [RR] To the best of your knowledge, what is the current physical impact[39] of this incident?
No impact
Damage to non-critical property
Damage to critical property[40]
Damage to non-critical systems
Damage to critical systems
Destruction of non-critical property
Destruction of critical property
Destruction of non-critical systems
Destruction of critical systems
Unknown

Economic Impacts to Entity

(DESIGN NOTE: NCISS Variable = Economic impact (NEW, not currently mapped in algorithm from reporter's response.)

[Op] + [RR] To the best of your knowledge, what is the current economic impact[41] of this incident? **(DISPLAY NOTE: Estimate any costs or losses associated with the categories of economic impacts listed below. If you require further clarity on the meaning of these categories of economic impacts, see the CISA report: "Cost of Cyber Incident."[42])**

Incident investigation and forensic analysis
Please provide estimates in U.S. dollars for each applicable category of economic impact (use a range from minimum to maximum where uncertain, or the same for both if known) **(DESIGN NOTE: Repeated for each selected)**
Incident response and containment (including direct response, cleanup, and recovery costs)
Lost revenue or productivity
Theft, fraud, and direct financial losses (including any ransomware payments disbursed)
Legal fees and regulatory fines
Victim notification and protection services
Other losses (e.g., loss of intellectual property)

Incident Details

32. Incident: Details by Stage

(DISPLAY NOTE: The following questions will collect details about the incident according to how far you are in the "incident lifecycle" (based on the major phases of an incident life cycle from NIST 800-61 r2, Computer Security Incident Handling Guide). [43] Please note, you can be in multiple stages of an incident response at one time and can revisit any incident stage-specific section of this report at any point if there is new information to report.)

Identification and Detection (I/D) Stage:

[RA] Provide a high-level summary of the incident. **(DESIGN NOTE: Open Text) (DISPLAY NOTE: Requests for more details will occur later in this report. Please provide a short "executive summary" of the incident**

---

[39] **Physical Impact**: The resultant of an incident that has caused intentional or accidental damage to a physical system/facility/surrounding environment, that disrupts, incapacitates, or destroys reliable operations of critical infrastructure, including personnel therein.

[40] **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. *Derived from "critical asset" page 135-136 and critically page 139 of https://www.dhs.gov/publication/dhs-lexicon*

[41] **Economic Impact**: Any costs or losses experienced due to an incident, including the general categories listed in this form in question #38A-G. These categories are more specifically defined in the CISA report: "Cost of Cyber Incident;" see Table 44 in Appendix C, https://www.cisa.gov/sites/default/files/2023-01/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf

[42] See Table 44 in Appendix C; https://www.cisa.gov/sites/default/files/2023-01/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf

[43] https://csrc.nist.gov/pubs/sp/800/61/r2/final

with a narrative of the incident detection. Consider including a description of any unauthorized access (including whether the incident involved an unattributed cyber intrusion), identification of any informational impacts or information compromise, any network location where activity was observed, and a high-level description of the impacted system(s) (e.g., "email servers, a network firewall, and a web server").)

[RA] Have you performed any incident response activities (e.g., cyber hunt activities) to determine the scope and impact of the incident? (Yes/No)
{Conditional} [Op] + [FISMA Req] **(DESIGN NOTE: If Yes)** Please explain and include any actions already taken as well as intelligence you may have learned to date **(DESIGN NOTE: Open Text)**
[RA] When was the incident first detected?
Detection date and time (yyyy-mm-dd HH:MM -<UTC offset>)

33. Incident Stage (I/D): Type Determination

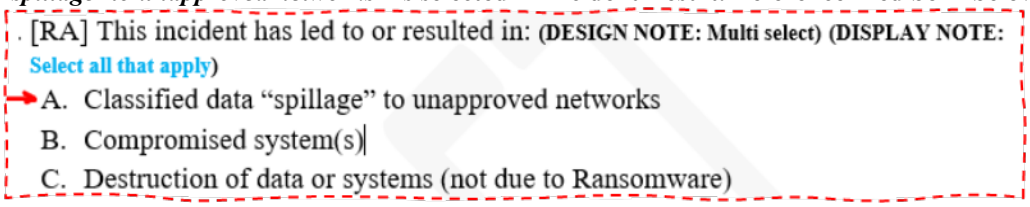
[RA] To the best of your knowledge, please select the categories involved in this incident **(DESIGN NOTE: Multi select, then drop down for more refined selections within each main category, dropdown lists are in Appendix 3.) (DESIGN NOTE: Must have the drop lists "searchable" by key words by type and subtype categories.) (DISPLAY NOTE: Select all that apply)**
Malware [e.g., ransomware, DDOS, etc.]
Human (or technology) errors [e.g., loss of equipment, system misconfiguration, mishandling of sensitive and/or PII documentation, etc.]
Hacking [e.g., password cracking, SQL injection, cross-site scripting, 'system' overflows, etc.]
Physical actions/destruction [e.g., sabotage, theft, etc.]
Environmental factors [e.g., fire, flood, etc.]
Social engineering [e.g., phishing, extortion, spam, etc.]
Misuse of assets (sometimes called "insider threats') [e.g., privilege abuse, unauthorized hardware/software, etc.]
[RA] This incident has led to or resulted in **(DESIGN NOTE: Multi select) (DISPLAY NOTE: Select all that apply)**
Classified data "spillage" to unapproved networks
Compromised system(s)
Destruction of data or systems (not due to ransomware)
Destruction of data or systems (via ransomware)
Defacement
Equipment loss: loss of control of physical equipment not from theft
Operational technology response functions inhibited (e.g., safety, protection, quality assurance, and operator intervention functions are prevented from responding to a failure, hazard, or unsafe state[44])
Operational technology process control impaired (e.g., physical control processes are manipulated, disabled, or damaged[45])
Supply chain customer disruption **(DISPLAY NOTE: The incident involved one of the reporting entity's vendors, with an impact on the reporting entity)**
Supply chain vendor disruption **(DISPLAY NOTE: The incident impacted a system or product that is supplied by the reporting entity to its customers, with a potential impact to one or more customer)**
Unauthorized account access
Unauthorized removal of account access (e.g., entity's system administrator's account deleted)
Unauthorized information access
Unauthorized release of information (virtually via computing systems) 46

---

https://csrc.nist.gov/pubs/sp/800/61/r2/final
TA0107/"Inhibit Response Function, Tactic TA0107 - ICS | MITRE ATT&CK®
[45] Impair Process Control, Tactic TA0106 - ICS | MITRE ATT&CK®
[46] Unauthorized release of information "virtually" is an occurrence where a person other than an authorized user potentially obtains the data, such as by means of a network intrusion, a targeted compromise that exploits website vulnerabilities, the inadvertent disclosure of information (including PII) via a public website, or a phishing or social engineering incident executed through an email message or attachment. It may also include an authorized user obtaining sensitive information (including PII) for other than the authorized purpose. If such an incident involves

Unauthorized release of information (physically via printed documents or physical media, or orally)[47]
Unauthorized use of information
Other [describe]

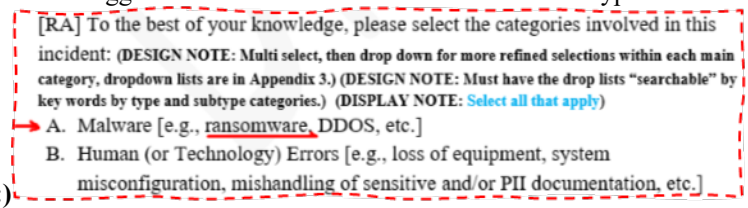
{Conditional}[FISMA Req + FedRAMP reporting only] **(DESIGN NOTE: Display only if *"Classified data 'spillage' to unapproved networks"* is selected in Incident Result. Reference "red box" below:)**



You indicated earlier that the incident resulted in spillage of classified information, please provide more details below (**DISPLAY NOTE: DISCLAIMER Do NOT provide any classified information in the following responses)**
What classification guide or source material was used to validate that the information spilled was classified?
What was the root cause of the spillage? **(DESIGN NOTE: Open text)**
[CUI]Has an appeal or challenge been issued on the spillage of classified information? (Yes/No)
On what date?
[CUI]To whom was the appeal or challenge issued?
Has the appeal been completed? (Yes/No)
Was this appeal accepted or denied? (Accepted/Denied)
If so, on what date was the appeal accepted or denied?

34. Incident Stage (I/D): Ransomware and Cyber Extortion:

(DESIGN NOTE: Executes if incident is flagged as a Ransomware Incident in "Incident Type Determination" above as indicated in "red box" below:)



35. Initial Ransom Demand Details:

[RC] Please provide the following details about the ransom demand associated with this incident:
[C-15] [Op] + [FISMA Req] Text of ransom demand(s) **(DESIGN NOTE: Open text)**
[C-15] [Op] + [FISMA Req] Screenshot of ransom note(s) or copy of the email(s)
[C-15] [Op] + [FISMA Req] Ransomware variant used (if known)
[C-15] [Op] + [FISMA Req] Amount of ransom demand
[C-15] [Op] + [FISMA Req] Currency type of ransom demand, including virtual currency
[C-15] [Op] + [FISMA Req] Text of ransom payment instructions (if not already included in response to A, above)
(DESIGN NOTE: Allow for a response to be "Same as response A", this is an open text otherwise.)

personally identifiable information (PII) on a federal system, the unauthorized release is considered a Breach per OMB – M-17-12. Often, an occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves PII.

[47] Unauthorized release of information "physically" is an occurrence where a person other than an authorized user potentially obtains the data due to the loss or theft of physical documents that include information (including PII), portable electronic storage media that stores information (including PII), or an oral disclosure of this sensitive information (including PII) to a person who is not authorized to receive that information. If such an incident involves PII on a federal system, the unauthorized release is considered a Breach per OMB – M-17-12. Often, an occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves PII, as is often the case with a lost or stolen laptop or electronic storage device. This result includes improper disposal of sensitive and/or PII documentation in containers that could be accessed by non-authorized personnel (e.g., information with customer credit card or social security numbers thrown in local dumpster or lost mail containing PII).

[C-15] [Op] + [FISMA Req] Deadline given to pay ransom. Please provide the Date and Time (yyyy-mm-dd HH:MM -<UTC offset>) **(DISPLAY NOTE: This could be a time in the future at time of report.)**
[C-15] [Op] + [FISMA Req] Description of any additional communications between the threat actors and either the impacted entity or a third party authorized to act on its behalf (e.g., phone conversations)
[Op] + [FISMA Req] Does your organization have insurance that covers ransomware demand payments? (Yes/No) **(DESIGN NOTE: If Yes)** Please provide insurance company details
Name
Email address
Unknown
Website
Unknown
Physical address
Street name and number
Postal code
City
State
Country
Other contact information
Insurance annual premium amount **(DISPLAY NOTE: Primary carrier amounts if applicable, and if there is a separate cost for "ransom payments" only include that amount, otherwise total cost is acceptable.)**
Amount
[ ] Select if primary carrier amount
[ ] Ransom coverage only [ ] Total coverage **(DESIGN NOTE: Select one)**
Does the impacted entity plan on seeking, or has it already sought coverage from its insurers for this incident? (Yes/No)

36. Ransom Payment Details

Ransom Payment Details
[Op] + [FISMA Req] Was a ransom paid? (Yes/No)
{Conditional} + [OP] + [RR] **(DESIGN NOTE: If Yes)** Did your ransom payment insurance cover the incident? (Yes/No) **(DESIGN NOTE: Only ask if answered "Yes" to having ransomware insurance and planning to seek coverage.)**
{Conditional} [Op] + [FISMA Req] If ransom was paid, provide the following **(DESIGN NOTE: Set Payment Count as 1.)**
(DESIGN NOTE: ========Ransomware Payment Details==========
[CUI] [Op] + [FISMA Req] **Negotiation Details:** Did you use a negotiation agent? (Yes/No), {Conditional} + [Op] + [FISMA Req] **(DESIGN NOTE: If Yes)** Provide
[CUI]Negotiation agent point of contact
[CUI]If person
First
Last
Phone number(s)
Email address(es)
Position/title
If entity
Name
Email address
Unknown
Website
Unknown
Physical address
Street name and number
Postal code
City

State
Country
Other contact information
(DISPLAY NOTE: When a ransom payment is made, the victim sharing information regarding the payer (the person paying the ransom payment), the recipient (the person receiving the ransom payment), and how the transaction occurred can enable a more effective federal response to a ransom (or extortion) incident. CISA recognizes there may be multiple transactions over the course of the incident; this form will solicit the (potentially) unique details for each transaction separately.)
[CUI] [Op] + [FISMA Req] Is the payer an individual or entity? (Select: Individual/entity) **(DESIGN NOTE: Single select)**
[CUI]{Conditional} + [Op] + [FISMA Req**]** [**Payer**] **(DESIGN NOTE: If Individual)**:
First
Last
Phone number(s)
Email address(es)
Position/title
Organization
[CUI]{Conditional} + [Op] + [FISMA Req] [**Payer**] **(DESIGN NOTE: If Entity)**:
Entity name
[CUI] Point of contact
First
Last
Phone number(s)
Email address(es)
Position/title
Entity email address
Unknown
Website
Unknown
Physical address
Street name and number
Postal code
City
State
Country
[CUI] Other contact information
[CUI] [Op] + [FISMA Req] [Payer] Details of transaction(s) per payment made to date: **(DISPLAY NOTE: This is from the Payer's perspective. Additionally, the total ransom/extortion amount could be spread among multiple payments and different methods.)**
Date payment was disbursed from the entity making the ransom payment to satisfy the ransom demand
Currency type (traditional, digital, or other)
Currency **(DESIGN NOTE: Based on the selection of currency type, the system will make the selections available for currency options)**
Other, provide description **(DESIGN NOTE: Open text)**
Amount of payment (may be equal to or different from the actual demand)
In digital asset
In US dollar value at the time of the transaction
[CUI] For transactions that involved a bank or another type of financial institution (e.g., in facilitating the payment)
Name of bank or financial institution
Address of bank or financial institution
Street name and number
Postal code
City

State
Country
Name(s) on the account
Account number
Routing number
Origin
[CUI] If virtual (e.g., crypto) currencies were used:
Service used to
Purchase the currency
Store the currency
Transmit the currency
[CUI] Transaction ID (e.g., transaction hash), if known
[CUI] Virtual (crypto) currency address(es)
Payer addresses
Other method of paying the ransom / extortion demands
[CUI] Describe the method
If the transaction occurred at a physical location, please provide
Address of transaction
Geographical point of interest (location)
Street name and number
Postal code
City
State
Country
Any other physical location characteristics describe here:
[CUI] [Op] + [FISMA Req] To the best of your knowledge, is the **recipient** an individual or entity/group?
Select: [ ]Individual [ ]Entity [ ]Group [ ]Unknown **(DESIGN NOTE: Skip "point of contact" info if "Unknown" selected) (DESIGN NOTE: Single select)**
[CUI] [Op] [FISMA Req if selected] [Recipient] **(DESIGN NOTE: If Individual)** Please provide the following information to the extent known:
First
Middle
Last
Suffix
Phone number(s)
Email address(es)
Social media information
Position/title
[CUI] [Op] + [FISMA Req if selected] [Recipient] **(DESIGN NOTE: If Entity/Group)** Please provide the following information to the extent known:
Name
[CUI] Point of contact at entity
First
Middle
Last
Suffix
Phone number(s)
Email address(es)
Position/title
Entity email address
Entity social media information
Entity website
Physical address

Street name
Street number
Postal code
City
State
Country
Any other contact information describe here:
[CUI] [Op] + [FISMA Req if available] [Recipient] Details of transaction(s) per payment: **(DISPLAY NOTE: This is from the Recipient's perspective. Additionally, the total ransom/extortion amount could be spread among multiple payments and different methods.)**
Date and time of ransom payment
Currency type (traditional, virtual/digital, or other)
Currency **(based on the selection of currency type, the system will make the selections available for currency options)**
Other, provide description **(DESIGN NOTE: Open text)**
Amount of ransom payment (may be equal to or different from the actual demand)
In virtual/digital asset
In US dollars
[CUI] For transaction(s) that involved a bank or another type of financial institution:
Name of bank or financial institution
Address of bank or financial institution
Street name and number
Postal code
City
State
Country
Name(s) on the account
Account number
Routing number
Destination
If virtual (e.g., crypto) currencies were used
Service used to
Purchase the currency
Store the currency
Transmit the currency
[CUI] Transaction ID (e.g., transaction hash), if known
[CUI] Virtual (crypto) currency address(es)
Payee addresses

[Op] + [FISMA Req] Identifying payment installments
Were multiple payments made (e.g., installments, differing methods [some physical cash, some virtual])? (Yes/No)
(Design Note: If Yes, complete another session of "payment details", associate payment # to installment # + 1. Provide an option to copy over from the first payment the information since it may be all the same except for date/time.)
(DESIGN NOTE:^^^^^^^^**=End of Ransom Payment Details=**^^^^^^^^)

37. Results of Ransom Incident

[CUI] [Op] + [FISMA Req] Results of ransomware/cyber extortion incident
Were you provided with decryption capabilities (e.g., keys) by the threat actor? (Yes/No)
(DESIGN NOTE: If Yes) Did the keys work?
What percentage of the files were recoverable (approximate)?
To the best of your knowledge, was any data stolen? (Yes/No/Unsure) **(DESIGN NOTE: If Yes or Unsure)**:
[CUI] Describe the type of data stolen or suspected to have been stolen, to the best of your knowledge **(DESIGN NOTE: Open text)**

[CUI] Did the threat actors leak any stolen data, to the best of your knowledge? (Yes/No) **(DESIGN NOTE: If Yes)** [describe]
[CUI] Did the threat actors use any other pressure tactics, such as contacting third parties to inform them of the compromise? (Yes/No) **(DESIGN NOTE: If Yes)** [describe].
[CUI] Describe any additional results of the ransom incident.
[Op] + [FISMA Req] Did you experience follow-on attempts by threat actors to extort money or services? (Yes/No)
{Conditional} [Op] + [FISMA Req] **(DESIGN NOTE: If Yes)** Did you pay the additional ransom or extortion demands? (Yes/No)
(DESIGN NOTE: If Yes, repeat **===Ransomware Payment Details==Set Payment Count as +1)**

[Op] + [FISMA Req] Do you have any other information regarding the ransomware incident not previously provided (e.g., communications with the threat actors, transcripts, audio recordings, emails, chats)? (Yes/No)
Describe **(DESIGN NOTE: If Yes: Open text) (DESIGN NOTE: Reporter should be able to go through and update the specific question that is relevant and has already been asked.)**

38. Incident Stage (I/D): Tactics, Techniques and Procedures (TTPs) and Indicators of Compromise (IOCs) Observed

[RA] Would you like to document the tactics, techniques, and procedures (TTPs) and related indicators of compromise(s) (IOCs) you observed by using our offline template and uploading the completed file, or would you prefer to proceed and enter the TTPs and IOCs directly in this online form?

(DESIGN NOTE: select one) (DESIGN NOTE: If "Template" is selected, provide file download link and instructions to the reporter for filling out the template of TTPs and IOCs and then, when done, provide instructions on how to upload the file and any validations that need to occur once the system has processed the data in the file)(DESIGN NOTE: If "Template" is selected, skip over following questions 47, 48, 49, 50).
[ ] I'd like to use the offline template **(DESIGN NOTE: If selected, proceed to Q46)**
[ ] I'd like to proceed with this report using the online form **(DESIGN NOTE: If selected proceed to Q47)**
{Conditional on Q45.A is selected} [Op] You have indicated you will use the offline template to document your TTPs and IOCs, then will upload the file once complete. Please proceed with the download of the template and instructions (below) and return to this point in the online form to upload your completed file.
Download the TTP/IOC template/instructions here: DOWNLOAD TEMPLATE/INSTRUCTIONS **(DESIGN NOTE: Provide guidance in the instructions to use CISA's internal tool to help understand what TTPs they have experienced. Possible integration with CISA's work on MITRE's DECIDER work to determine the correct ATT&CK TTPs. (https://www.cisa.gov/resources-tools/resources/decider-fact-sheet))**
Upload the completed TTP/IOC file offline template here: UPLOAD TEMPLATE **(DESIGN NOTE: There needs to be a validation mechanism in place to: 1. Acknowledge a file upload had occurred. 2. Validate the file is organized in the format prescribed in the template and instructions. 3. Display the content once available to the reporter to validate and edit one imported into the incident report.)**
Select **here** to continue this report and return to upload your offline form later **(DESIGN NOTE: provide "button" and method to skip over questions 47, 48, 49, 50 and go to Q 51 in the *"Incident Stage (I/D): Indicators of Compromise (IOCs): Detection Methods"* section)**

39. Incident Stage (I/D): Tactics, Techniques and Procedures (TTPs) Observed

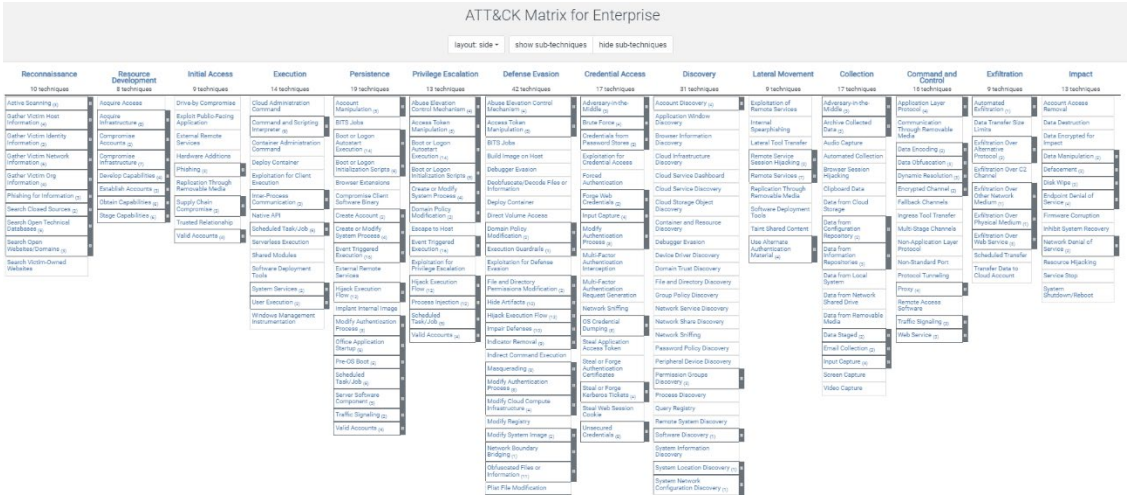
{Conditional on Q45.B is selected} + [RA] You have indicated you want to document your TTPs and IOCs directly into this form. At this time, can you provide information regarding the TTPs the adversary leveraged as part of this incident? (Yes/No) **(DESIGN NOTE: If No: DISPLAY NOTE: When, during your investigation, you discover knowledge about TTPs contributing to the incident, please return to this question and document them. If you have already documented and IOCs, you must also return to that section and provide the connections between the IOCs and TTPs documented that have factored into the incident.) (DESIGN NOTE: Proceed to Q49. This means there is a possibility to document IOCs without first documenting any TTPs)**
{Conditional}[RC] **(DESIGN NOTE: Question applies only if "Yes" to TTPs to report [Q47] and selection of "Proceed directly in report" to documenting TTP/IOC in Q45.B)** You have indicated you have TTP(s) to report and would like to document those TTP(s) and related IOC(s) directly in this online form. Therefore, please begin by

selecting the type(s) of networks[48] and systems the TTPs were observed within. (Select all that apply). [ ] Enterprise/Traditional IT; [ ] Operational Technology/Industrial Control Systems; [ ] Mobile Systems **(DESIGN NOTE: Multi select)**
Are you familiar with the MITRE ATT&CK TTP framework? (Yes/No) **(DESIGN NOTE: Reporter must answer at least one of the following two questions, either MITRE ATT&CK selection or the "tactic category with narrative" option but can also select both if applicable to enter TTPs in both MITRE format and a narrative for more than one TTP if they have one or more in both categories. Allow for different combinations for 1 or more TTP in both MITRE format and the narrative format):**

Would you like to use CISA's internal tool to help you understand what TTPs you experienced? (Yes/No)
(DESIGN NOTE: If Yes, Possible integration with CISA's work on MITRE's DECIDER work to determine the correct ATT&CK TTPs. (https://www.cisa.gov/resources-tools/resources/decider-fact-sheet)**)**
(DESIGN NOTE: If Yes AND if No to "familiar with MITRE ATT&CK") Once you have completed using CISA's internal tool to help understand your TTPs, are you now able to use MITRE ATT&CK framework to identify your TTPs? (Yes/No)

(DESIGN NOTE: If Yes to "familiar with the MITRE ATT&CK" or Yes after using CISA's internal tool)
{Conditional} [Op] + [FISMA Req] Select the appropriate MITRE ATT&CK tactics and/or technique(s) observed from the matrix associated with the network(s) you have selected
One or more TTPs observed in this incident are not identified in MITRE ATT&CK, therefore we need to document those TTPs in a different method. [ ] Select if applicable **(DESIGN NOTE: If selected allow for a combination of both MITRE ATT&CK TTP and alternate narrative method TTP identifications)**
(DESIGN NOTE: This list of Enterprise, Mobile, and ICS attack vectors is derived from MITRE ATT&CK's TTPs. This should be a multi select and expanding option list given choice selected at the Enterprise, Mobile, and ICS levels.)
(DESIGN NOTE: After choosing between the Enterprise, Mobile, and ICS Matrices: (see https://attack.mitre.org/matrices/ for MITRE ATT&CK lists.) The recommendation is to display similar to the actual MITRE ATT&CK matrices for a visual navigation (expectation is that the type of incident/compromise previously identified will map to the appropriate MITRE ATT&CK tactics, at a MINIMUM. The reporter can add tactics as identified and necessary.) NCISS Variable = Observed Activity this is covered now in the MITRE ATT&CK TTP section(s) (BACKEND and NCISS Variable Design Note: This MITRE ATT&CK is replacing the ODNI "Observed Activity Characterization.") For intermediate NCISS Score mapping, each of the MITRE ATT&CK technique headings (i.e., Recon, Initial Access) needs to be bucketed into one of the legacy ODNI categories of: [Preparation, Engagement, Presence, or Effect/Consequence] (e.g., Recon, Initial Access = Preparation) and inherit those appropriate NCISS values.)

Enterprise Networks: Networks and systems that consist of and/or support information for the following platforms: Windows, macOS, Linux, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network management devices (e.g., routers, switches, hubs, etc.), and Containers.
Industrial Control Networks: Operational Technology are programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. (Operational technology - Glossary | CSRC (nist.gov))
Mobile Device Networks: Mobile devices/networks that have access to entity resources and network-based effects that can be used by adversaries. This includes supported devices for the following platforms: Android, iOS.



{Conditional} [Op] + [RR] **(DESIGN NOTE: If "no" to familiar with MITRE ATT&CK)** You have indicated you are unfamiliar using MITRE ATT&CK to identify TTPs observed used during this incident, or your entity observed TTP(s) not listed or that is currently unidentified in MITRE ATT&CK. Therefore, using the type of network(s) you have selected earlier, please select the TTP category that potentially matches the type of TTP you have observed: **(DESIGN NOTE: Depending on which network selected earlier (Enterprise, ICS, Mobile) display the TTP category list (defined in "red box" below) for each type of network and allow reporter to select one to many categories and allow a description narrative for each category chosen) (DESIGN NOTE: Provide "hover-over" descriptor of each category in each list to provide context/descriptor for the reporter.)**

Enterprise Networks	Mobile Networks	Industrial Control Systems
Reconnaissance	Initial Access	Initial Access
Resource Development	Execution	Execution
Initial Access	Persistence	Persistence
Execution	Privilege Escalation	Privilege Escalation
Persistence	Defense Evasion	Evasion
Privilege Escalation	Credential Access	Discovery
Defense Evasion	Discovery	Lateral Movement
Credential Access	Lateral Movement	Collection
Discovery	Collection	Command and Control
Lateral Movement	Command and Control	Inhibit Response Function
Collection	Exfiltration	Impair Process Control
Command and Control	Impact (physically to data/systems)	Impact (physically to data/systems)
Exfiltration		
Impact (physically to data/systems)		

i. Please provide a description and details of the TTPs observed in the category(ies) you have documented **(DESIGN NOTE: Open text box) (DESIGN NOTE: Possible integration with CISA's work on MITRE's DECIDER work to determine the**

correct ATT&CK TTPs. (https://www.cisa.gov/resources-tools/resources/decider-fact-sheet))

40. Incident Stage (I/D): Indicators of Compromise (IOCs) and associated Detection Methods Used

(DISPLAY NOTE: In the next series of questions, you will be asked to provide Indicators of Compromise (IOCs) details and metadata observed and collected for each TTP selected.)
[C-15] [RA] Do you have any Indicators of Compromise (IOCs) you can share with us? (Yes/No) **(DISPLAY NOTE: You will be given an opportunity to associate reported IOC(s) with your entity's documented TTP(s) in a future step. (DESIGN NOTE: IF No: SKIP to Q52, the "Incident Stage (I/D): Malware Artifacts and Detection Logics/Analytics" section)**
(DESIGN NOTE: If Yes) There are two methods by which you can share IOCs with us. Option one is via a "copy/paste" of your IOC(s) into this form with opportunities to add additional IOC attributes once the system processes your "copy/paste". Option two is via providing the IOC(s) individually in a structured format wherein you provide attribute details and TTP mapping at the time of entry. **(DISPLAY NOTE: Based on previous incident reporting and our experience, if there are 10 or fewer IOCs to report, the structured "individual build" approach may be the best option to document the IOCs.)** Which method do you want to use to document your IOC(s)? [ ] "Copy/paste; [ ] "Individual build"**(DESIGN NOTE: Can be multi select for reporter to bulk upload some IOCs and if they prefer, to individually document other IOC(s).)**

[RC] **(DESIGN NOTE: Show option if "Copy/paste" option selected) (DISPLAY NOTE: To ensure we can ingest your data correctly you will need to provide your IOCs separated by a space, comma, semicolon, or new line.)** Provide your IOC(s) via copy/paste here **(DESIGN NOTE: Open text box) (DESIGN NOTE: For Data marking: Reporter needs the opportunity to label the IOC information as proprietary at some point, e.g., through data markings/options to be marked in the CISA 2015 section)**
Upload via copy/paste method
IOC Relation; Type; Context, Timeline [Start, Stop, Still ongoing (Y/N)]; IOC location observed [from NCISS "pick list"
(DESIGN NOTE: Provide validation for reporter: redisplay reporter's input, allow for immediate correction edits by reporter) Please validate and edit any errors to your IOC(s) here
Based on the current IOC list reported, it is very helpful to CISA if you can provide additional context on the IOCs. The context which is particularly valuable to us is an explanation of whether the indicator is from the attacker, benign, unknown, the times seen, if the IOC is currently active in your environment, and the location the IOC was operating from within your network(s). It is preferred to have the attributes associated per individual IOC. At a minimum, the attributes can be applied to all IOCs of the same type. At what level are you able to provide us context on the IOC(s) you are sharing? [ ] Attributes per IOC entry [ ] Attributes per IOC type (Select one) **(DESIGN NOTE: Single select)**
(DESIGN NOTE: If "Attributes per IOC entry" selected: provide method to add the following attribution values to each IOC provided and parsed as an individual entry. Use the same attribute values for each IOC.)
Based on the IOC(s) added to your report, please provide the overall IOC attributes as necessary:
Were these IOCs [ ]Attacker, [ ]Benign, [ ]Unknown (Select all that apply) **(DESIGN NOTE: multi select)**
Please provide the timeline of the IOC(s) collected
First known time IOC operational in your environment
Is the IOC still active in your environment? (Y/N) **(DESIGN NOTE: If No)**
Time IOC ceased operation within your environment
Please select (one) the most severe location any of the IOCs were operating from within your environment from this list:
Business demilitarized zone (DMZ) (Activity was observed in the business network's demilitarized zone (DMZ))
Business network (Activity was observed in the business or corporate network of the victim; these systems would include corporate user workstations, application servers, and other non-core management systems)
Business network management (Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores)

Critical system[49] DMZ (Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay "jump" boxes into more critical systems.)
Critical system management (Activity was observed in high-level critical systems management such as human-machine interfaces in Industrial Control Systems)
Critical systems (Activity was observed in the critical systems that operate critical processes.)
Unknown
Other [describe] **(DESIGN NOTE: Open Text)**
(DESIGN NOTE: If "Attributes per IOC type" selected: provide method to add the following attribution values to each IOC provided and parsed as an individual entry. Use unique attribute values for <u>each</u> IOC.)
Based on each of the IOCs added to your report, please provide the individual IOC attributes as necessary
Was the IOC [ ]Attacker, [ ]Benign, [ ]Unknown (Select one) **(DESIGN NOTE: Single select)**
Please provide the timeline of the IOC provided
First known time IOC operational in your environment
Is the IOC still active in your environment? (Y/N) **(DESIGN NOTE: If No)**
Time IOC ceased operation within your environment
Please indicate any of these areas or locations in your organization's network(s) where you observed the IOC (select all that apply) **(DESIGN NOTE: select from NCISS "Location pick list" for IOC(s) location) (DESIGN NOTE: NCISS Variable = Location of Observed Activity NCISS "Location pick list" for IOC(s) location)**
Business demilitarized zone (Activity was observed in the business network's demilitarized zone [DMZ])
Business network (Activity was observed in the business or corporate network of the victim; these systems would include corporate user workstations, application servers, and other non-core management systems)
Business network management (Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores)
Critical system[50] DMZ (Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay "jump" boxes into more critical systems.)
Critical system management (Activity was observed in high-level critical systems management such as human-machine interfaces in Industrial Control Systems)
Critical systems (Activity was observed in the critical systems that operate critical processes.)
Unknown
Other [describe] **(DESIGN NOTE: Open Text)**
Please associate the IOC(s) you provided with the appropriate TTP(s) you have already documented. If you have not yet documented any TTPs, please select [here] to omit this step for now. **(DESIGN NOTE: if reporter selects "[here]" allow the IOC to TTP mapping process to be postponed and DISPLAY NOTE: When, during your investigation, you discover knowledge about TTPs contributing to the incident and have documented them, please return to this question and provide the associations between the IOCs and TTPs documented that have factored into the incident) (DESIGN NOTE: Select from TTP entered "pick-list" and allow reporter to associate the IOC as they are individually parsed from mass template upload with TTP(s))**
Individual build method **(DESIGN NOTE: For Data marking: reporter needs the opportunity to label the following IOC information as proprietary at some point, e.g., through data markings/options to be marked in the CISA 2015 section.)**

[49] **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. *[derived from "critical asset" page 135-136 and critically page 139 of https://www.dhs.gov/publication/dhs-lexicon*
[50] **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. *[derived from "critical asset" page 135-136 and critically page 139 of https://www.dhs.gov/publication/dhs-lexicon*

Please select the TTP with which these IOCs are associated. **(DESIGN NOTE: if reporter selects "[here]" allow the IOC to TTP mapping process to be postponed and DISPLAY NOTE: When, during your investigation, you discover knowledge about TTPs contributing to the incident and have documented them, please return to this question and provide the associations between the IOCs and TTPs documented that have factored into the incident.) (DESIGN NOTE: Select from TTP entered "pick-list" and allow reporter to associate the IOC with a TTP.)**
(=======DESIGN NOTE: This section is repeated for each type of IOC the reporter is providing =====)
[Op] + [RR] What is the IOC's relation to the incident? (Attacker, Benign, Unknown) **((DESIGN NOTE: Select one)**
[C-15] [Op] + [RR] Select type of indicator of compromise **(Select from list:)**:
Autonomous System(s) (AS)
Domain Name(s)
Email Address(es)
Email Message(s) **(DESIGN NOTE: Allow option to upload Email Headers separate from Email Body.)**
IPv4 Address(es)
IPv6 Address (es)
Network Traffic
URL
File System Directory(ies)
File Metadata
Hash(es)
Mutex(es)
Software Metadata
System Process(es)
User Account(s)
Windows Registry
X.509 Certificate(s)
[C-15] + [RA] Please share any relevant context regarding these IOCs **(DESIGN NOTE: Open text)**
[Op] + [RR] Please enter your IOC timeline here
First known time IOC operational in your environment
Is the IOC still active in your environment? (Y/N) **(DESIGN NOTE: If No)**
Time IOC ceased operation within your environment
[C-15] + [Op] + [RR] Please indicate any of these areas or locations in your organization's network(s) where you observed the IOC (select all that apply)
(DESIGN NOTE: NCISS Variable = Location of Observed Activity NCISS "Location pick list" for IOC(s) location)
Business demilitarized zone (Activity was observed in the business network's demilitarized zone [DMZ])
Business network (Activity was observed in the business or corporate network of the victim; these systems would include corporate user workstations, application servers, and other non-core management systems)
Business network management (Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores)
Critical system[51] DMZ (Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay "jump" boxes into more critical systems.)
Critical system management (Activity was observed in high-level critical systems management such as human-machine interfaces in Industrial Control Systems)
Critical systems (Activity was observed in the critical systems that operate critical processes.)
Unknown

[51] **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. *[derived from "critical asset" page 135-136 and critically page 139 of https://www.dhs.gov/publication/dhs-lexicon*

Other [describe] **(DESIGN NOTE: Open Text)**

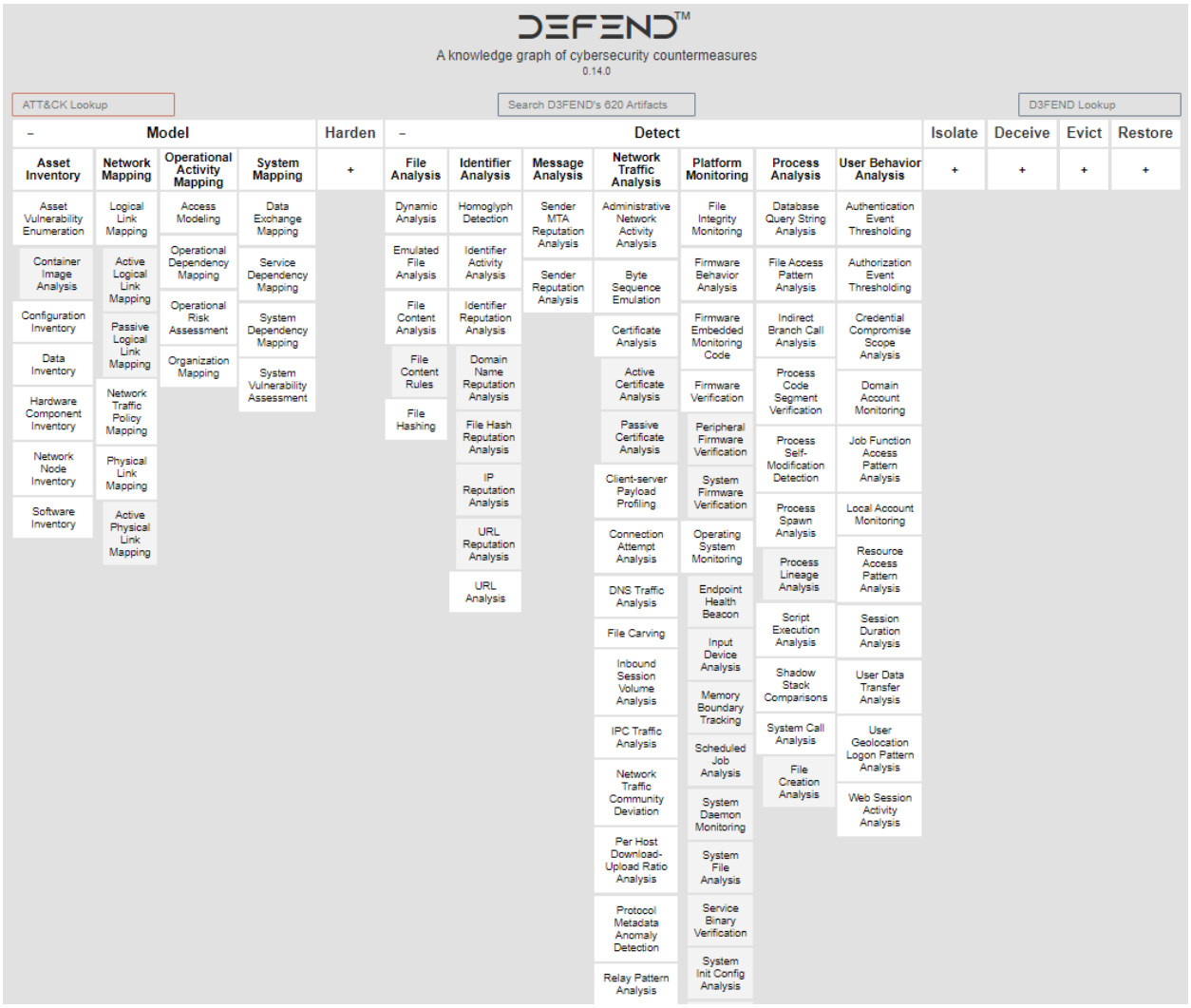
41. Indicator of Compromise (IOC) Individual Data Marking

(DESIGN NOTE: For Data Marking: reporter needs the opportunity to label the following IOC information as proprietary at some point, e.g., through data markings/options to be marked in the CISA 2015 section.) Should the IOC(s) and associated detail you have provided in this section be considered commercial, financial, and proprietary under the Cybersecurity Information Sharing Act of 2015? [Yes/No]

42. Incident Stage (I/D): Indicators of Compromise (IOCs): Detection Methods

[Op] + [RR] MITRE's D3FEND matrix categorizes countermeasures into multiple categories. Detection actions are identified in the "Model" and "Detect" categories. Are you familiar with, and/or would you like to use MITRE D3FEND matrix to document your detection methods? (Yes/No)

a. **(DESIGN NOTE: If yes)** Please select the detection methods you used to discover each observed activity IOC using the MITRE D3FEND matrix **(DESIGN NOTE: Display of this section to be similar to that of MITRE D3FEND site) (see https://d3fend.mitre.org/ for MITRE D3FEND list. The recommendation is to display similar to the actual MITRE D3FEND matrix(ces) for a visual navigation) (DESIGN NOTE: Select all that apply = this question is designed to be on a loop for as many counter measures reported.) (DISPLAY NOTE: Please return to this section at any point during the life cycle of this incident to document any additional detection methods used to help resolve this incident)**



b. **(DESIGN NOTE: If No) (DESIGN NOTE: Multi select)**

1. Did your organization choose a detection technique that potentially fit within an existing "MITRE D3FEND tactic" but was not listed? (Yes/No)

I. **(DESIGN NOTE: If Yes)**:

1. Which tactic did your action fall under?

a. Model

1. Asset inventory
2. Network mapping
3. Operational activity mapping
4. System mapping

b. Detect

1. File analysis
2. Identifier analysis
3. Message analysis
4. Network traffic analysis
5. Platform monitoring
6. Process analysis
7. User behavior analysis
8. Description **(DESIGN NOTE: Open text)**

II. **(DESIGN NOTE: If No)** If your organization is unable to use MITRE D3FEND, did not use any of the MITRE D3FEND detection methods, or is unsure which MITRE D3FEND detection method applies, select from the set of common detection methods below:
    1. Administrator
    2. Antivirus software
    3. Commercial and/or publicly available solution
    4. External source notification
    5. Human review
    6. Internally developed/proprietary solution
    7. Intrusion detection system (IDS)
    8. Log review
    9. User
    10. Unknown
    11. Other
        a. Please provide a description of the detection method(s). **(DESIGN NOTE: Open text)**

43. Incident Stage (I/D): Malware Artifacts and Detection Logics/Analytics

(DESIGN NOTE: For Data marking: reporter needs the opportunity to label the following Malware detection information as proprietary at some point, e.g., through data markings/options to be marked in the CISA 2015 section.)

[C-15] [RA] Did you detect malicious software (malware) or scripts? (Yes/No)
{Conditional} [Op] + [RR] **(DESIGN NOTE: If Yes)** Do you have any malware you can share with us? (Yes/No)
(DESIGN NOTE: If Yes) Please upload here **(DESIGN NOTE: If Yes, Option to submit via CISA's MALWARE=-ingest system here)**
[C-15] {Conditional} [Op] + [RR] **(DESIGN NOTE: If Yes)** Please provide any additional detail or context regarding the malware you have shared with us **(DESIGN NOTE: Open text)**

[Op] + [RR] Did you create any signatures or other detection analytics to identify and/or detect the threat activity you have reported? (Yes/No)
{Conditional} [Op] + [RR] **(DESIGN NOTE: If Yes)**
For each entry, please provide the following
Description
Pattern or rule
Pattern or rule language or technology used (Yara, Snort, SIGMA, etc.)

44. Incident Stage (I/D): Malware Artifacts and Detection Logics/Analytics: Data Classification Markings

[CUI] [Op] + [RR] The default data marking for the malware artifacts and detection logic/analytics just reported is {insert default data marking here, default data marking is TBD}. Would you like to change the default data marking? (Yes/No) **(DISPLAY NOTE: The default marking with the lowest restriction available will be applied to fields not previously entered with a data marking label automatically to all submissions in the Malware Artifacts and Detection Logics/Analytics sub-section. Although you will be given an opportunity to change the markings for responses to individual questions.)**
{Conditional} [Op] + [RR] **(DESIGN NOTE: If Yes)** Which of these data markings best describe your malware artifacts and detection logics/analytics?
(DESIGN NOTE: S**ee Appendix 1 for options.)**

45. Incident Stage (I/D): Data Sources Used and Attribution:
46. Data Sources Used

[Op] + [RR] Were external data sources such as data from threat information/intelligence reporting used to discover or aid in discovering this incident? (Yes/No) **(DESIGN NOTE: Provide ability to add more than one data source if needed)**
[If Yes]Provide the following for each data source
[Op] + [FISMA Req] Report title and number (if applicable)
Name/description of data source (can include author, company providing the data source, or general description)

Link to report/data source (if applicable and available to share)

47. Attribution

[RA] Have you attributed this incident to a threat actor? (Yes/No, This incident is currently an unattributed cyber intrusion/Maybe)
{Conditional} [Op] **(DESIGN NOTE: If Yes or Maybe)** Provide the name of the "threat actor" and the source used to support this assessment below
[ ] The attributed threat actor name and/or attribution source is classified (select if true) **(DESIGN NOTE: Flag incident for follow up with reporter on attribution claims if selected)**
DISPLAY NOTE: If you used a classified source to help in your attribution, do not complete the following. You will be contacted via a secure means to discuss further if necessary)
Threat actor name (could be name of advanced persistent threat [APT] actor, ransomware group, etc.) **(DESIGN NOTE: Open text)**
Was this attribution claim based on one of the data sources you previously provided? **(DESIGN NOTE: Allow to select from list (one to many entries.))**
If not, please provide the attribution source(s) **(DESIGN NOTE: One to many entries.)**
Name of attribution source(s) **(DESIGN NOTE one to many entries.)**
URL/Web link to validate source material **(DESIGN NOTE: One to many entries.) (DESIGN NOTE: Open text)**
Report title(s) and number(s) (if applicable) **(DESIGN NOTE: One to many entries) (DESIGN NOTE: Open text)**
Other details **(DESIGN NOTE: One to many entries.) (DESIGN NOTE: Open text)**
What is your level of confidence[52] in your attribution **(DESIGN NOTE: Select one)**
Confirmed by other sources: confirmed by other independent sources; logical in itself; consistent with other information on the subject
Probably true: not confirmed; logical in itself; consistent with other information on the subject
Possibly true: not confirmed; reasonably logical in itself; agrees with some other information on the subject
Provide any additional information you feel is relevant **(DESIGN NOTE: Open text)**

{Conditional} [Op] + [RR] **(DESIGN NOTE: If No)** This incident is currently an unattributed cyber intrusion. Please provide any additional information you feel is relevant and will aid in attribution. **(DESIGN NOTE: Open text)**
Assistance

48. Assistance from CISA

[Op] + [RR] Are you interested in receiving incident response assistance from CISA to the extent available? (Yes/No)
(DESIGN NOTE: If Yes, display links/descriptions for CISA's free on-demand services [TBD]: On-demand services CISA offers (service catalog link here).)
[Op] + [RR] Are you interested in additional collaboration or information sharing with CISA around this incident to the extent feasible? (Yes/No)
(DESIGN NOTE If Yes, add hyperlink to CISA "packaged help" [TBD], potential connect with local CSA.)

49. **Third Party Assistance**

[Op] + [RR] Are you utilizing an external third party to provide assistance with the reported incident? (Yes/No)
(DESIGN NOTE: If Yes) Provide the name of third-party entity(ies) **(DESIGN NOTE: Open text)**

50. Data Sharing and Logging Readiness

[OP] + [RR] Are you willing to share the results of third-party analysis with CISA? (Yes/No) **(DESIGN NOTE: Only Display if "Yes" to "contracting out assistance" question prior.)**
[OP] + [RR] Are you willing to share data (such as logs or other technical artifacts) about this incident with CISA? (Yes/No)
{Conditional} [Op] + [FISMA Req] [If Yes] Please select all categories of data (such as logs or other technical artifacts) you are willing to provide. If necessary, our request for logs and technical artifacts would encompass only

[52] https://www.misp-project.org/taxonomies.html#_admiralty_scale
https://www.threat-intelligence.eu/methodologies/

information related to the incident **(DESIGN NOTE: Multi select) (DISPLAY NOTE: You are not being asked to share this data with CISA at this time/through this report. The purpose of this question is for CISA to understand the extent to which such data exists, and you are willing to share it with CISA for potential analysis.)**
Identity-based logs for the following
Identity and credential management
Privileged identity and credential management
Authentication and authorization
User accounts and user account meta-data
Network
Email filtering, spam, and phishing logs
Network device infrastructure logs (for devices with multiple interfaces: interface MAC if correlated to the De-NAT IP address)
Network device infrastructure logs (e.g., general logging, access, authorization, and accounting)
Data loss prevention logs
Network traffic (e.g., packet capture) artifacts
Network traffic (e.g., Netflow, Enhanced Netflow, Zeek Logs, etc.) artifacts
Host:
Operating systems (e.g., Windows infrastructure and operating systems, MacOS, BSD)
PKI and other multifactor applications and infrastructure
Antivirus and behavior-based malware protection
Other host logs (e.g., operating system, database logs, application logs)
Vulnerability
Vulnerability assessments
Penetration test results
Mobile
Mobile (phones and tablets) EMM (UEM) / MTD server logs
Mobile (phones and tablets) EMM (UEM) / MTD agent logs
Containers:
Container (e.g., supply chain, image, engine (MGT/orchestration, OS, cluster/pod events)
Cloud unique data not specified above
Cloud environments (general events and general logging)
System configuration and performance
Virtualization systems
Mainframes
Mainframe unique logging not covered above
Communications
Any communications with the threat actors (either by the entity or another entity on behalf of the entity) (e.g., emails [with full headers and attachments], chats, etc.)
Notes, transcripts, and audio recordings of any communications with threat actors
Financial
Any log files supporting financial records and accounts associated with the incident **(DISPLAY NOTE: This is not intended to include actual financial account information, e.g., account numbers, etc.)**
Forensic images:
Forensic images (e.g., full disk, system, volume etc.) relevant to the incident
Memory images relevant to the incident
Malicious code
Malicious code and associated files related to the incident
Exfiltrated data
Data and metadata exfiltrated related to the incident (**DISPLAY NOTE: This is not intended to include actual compromised data.)**
Evidence of data and metadata exfiltrated, related to the incident
Reporting

Forensic and other reporting related to or concerning the incident (internal or external party originated)

Analysis Stage[53] (A)
[RA]Have you begun the analysis stage? (Yes/No/Unsure) **(DISPLAY Note: The focus in this stage is on analyzing the incident in more detail, determining the root cause, and assessing the impact.)**
(DESIGN NOTE: If Yes) Please provide the date (yyyy-mm-dd) you began the analysis stage
[FISMA Req] Has the suspicious activity been declared an incident? (Yes/No) **(DISPLAY NOTE: This event and time is different from the first time of incident detection. An incident declaration is the point when your organization has officially analyzed the information and determined the activity detected is, in fact, evidence of a cyber incident.)**
(DESIGN NOTE: If Yes) Provide date and time (yyyy-mm-dd HH:MM -<UTC offset>) the incident was declared

51. Incident Stage (A): Impacted Users and Systems

[RA] Please identify the impacted users (number of impacted privileged and/or standard information technology (IT) users) **(DISPLAY NOTE: This is not necessarily all users, but those users impacted by activity during the incident.) (DESIGN NOTE: Multi select then quantity entered.)**
Privileged/system/administrative/service-level IT user quantity impacted **(DESIGN NOTE: Quantity)**
[Op] How are these users impacted (e.g., accounts locked, removed, other)?
Standard IT user quantity impacted **(DESIGN NOTE: Quantity)**
[Op] How are these users impacted (e.g., accounts locked, removed, other)?
[C-15] [RA] With respect to information systems you own and/or operate that are impacted by or involved in this incident: **(DESIGN NOTE: These set of questions repeat for every "instance" of Impacted Systems identified below.)**
[C-15] [RA] Identify and describe the function of each individual (or group of similar) affected network(s), device(s), and/or Information System(s), specifically with respect to the category, system type, services provided, name, location and government customer communities supported
Category (Select all that apply) **(DESIGN NOTE: Multi select)**
[ ]Enterprise networks or systems[54]: Impacted [confirmed] [suspected] (Select one) **(DESIGN NOTE: Single select)**
[ ]Operational technology[55] and industrial control systems: Impacted [confirmed] [suspected] (Select one) **(DESIGN NOTE: Single select)**
[ ]Mobile devices[56]: Impacted [confirmed] [suspected] (Select one) **(DESIGN NOTE: Single select)**

Systems type **(DESIGN NOTE: Multi select then quantity entered) (DESIGN NOTE: Modify drop lists accordingly per system category above, [e.g., if mobile device is selected, don't include options for "desktops" as an endpoint device])**
Endpoint devices (non-server devices)

---

[53] Analysis Stage - Stage of an incident life cycle that involves a process of examining [the systems] in terms of [but not limited to] their operation, configuration, and physical presence, in terms of "its constituent parts so as to reveal new meaning by investigation of the [system] elements to distinguish problems, situations, or anomalies for instructional solutions or other suitable interventions that optimize performance." Entering in the Analysis phase involves the transition from 'Something Happened' [Identification and Detection] to understanding 'What has Happened'. [derived from page28 of https://www.dhs.gov/publication/dhs-lexicon]

[54] Networks and systems that consist of and/or support information for the following platforms: Windows, macOS, Linux, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network management devices (e.g., routers, switches, hubs, etc.), and Containers.

[55] Operational Technology are programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. (Operational technology - Glossary | CSRC (nist.gov))

[56] Mobile devices that have access to entity resources and network-based effects that can be used by adversaries. This includes supported devices for the following platforms: Android, iOS.

Authentication token or device
Operating systems (OS) **(DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option selected)**
OS name(s)
OS version number(s)
Number impacted of each OS version
Desktop
Laptop
Media (e.g., backup tapes, disk media (e.g., CDs, DVDs), documents, flash drive or card, hard disk drive, media player, recorder)
Mobile phone or smartphone
Peripheral (e.g., printer, copier, fax, identity smart card, payment card (such as a magstripe or EMV))
Point of sale (POS) terminal
Tablet
Telephone
Voice over Internet Protocol (VoIP) phone
Other/unknown **(DESIGN NOTE: Open text)**
Server types
Active Directory (AD) Components
Operating systems (OS) **(DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option selected)**
OS name(s)
OS version number(s)
Number impacted of each OS version
Certificate Authority (CA)
Domain Name System (DNS)
Dynamic Host Configuration Protocol (DHCP)
Email
File
File Transfer Protocol (FTP)
Kerberos
Lightweight Directory Access Protocol/Lightweight Directory Access Protocol over Secure Sockets Layer (LDAP/LDAP[S])
Network Time Protocol (NTP)
Print
Remote log(s) (e.g., email, VPN, Syslog, R-Syslog, Syslog-NG)
Remote Shell (RSH)
Security Information and Event Management (SIEM)
Secure Shell (SSH)
TELNET
Virtual Private Network (VPN)
Web
Voice over Internet Protocol (VoIP) Gateways
Authentication, Authorization, and Accounting (AAA) Services (e.g., Radius, Terminal Access Controller Access-Control System [TACACS+])
Operational (OT) and Open-Source Software (OSS) types (e.g., Apache HTTP Server)
Other
Please list the additional server type(s) **(DESIGN NOTE: Open text)**
Network Devices
Firewalls
Operating systems (OS) (1.i, ii and iii. repeated for each selected)
OS name(s)
OS version number(s)
Number impacted of each OS version
Intrusion Detection System (IDS)

Intrusion Protection System (IPS)
Hub
Load Balancers
Proxies
Routers
Switches
Other
Please list the additional network device type(s) **(DESIGN NOTE: Open text)**
Identity providers (IdP)
Active Directory
Active Directory Federation Services (ADFS)
Amazon
Azure Active Directory
Facebook
Google Workspace
Lightweight Directory Access Protocol (LDAP)
Login.gov
Ping Federate
OpenID Connect
Provide the name of the provider(s) **(DESIGN NOTE: Open text)**
Okta
Security Assertion Markup Language (SAML)
Provide the name of the provider(s) **(DESIGN NOTE: Open text)**
Other identity providers
Please provide the name of the identity provider(s) **(DESIGN NOTE: Open text)**
Name of system(s) **(DISPLAY NOTE: Provide name of system to add fidelity to the system (or group of systems) that is entered in this instance (e.g., clarifying names of servers.)) (DESIGN NOTE: Open text)**
Name of system(s) services provided (e.g., active directory, email, web, boundary firewall, key personnel mobile device) **(DESIGN NOTE: Open text)**
Physical location(s) of system or group of systems
[ ] Select if same as impacted facility address entered earlier
(DESIGN NOTE: Display impacted facility address(s) from earlier and allow reporter to confirm or not if systems are located in same address and select.)
If not the same address as impacted facility, then please provide address of impacted system(s)
Street name and number
City
State
Postal code
Country
Is the impact or involvement of the system (or group of systems) identified [] confirmed or [] suspected at the time of report? **(DESIGN NOTE: Select one.)**

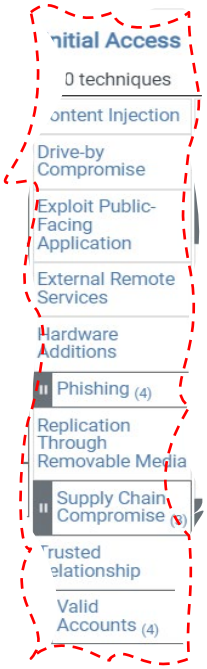
[FISMA Req] + [FedRAMP] Please identify whether any impacted information system, network, and/or device supports any elements of the intelligence community or contains information that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in 42 U.S.C. 2014(y) (Yes/No).
(DESIGN NOTE: This question is to flag for CISA to conduct notifications to the affected communities per EO 14028)
(DESIGN NOTE: If Yes) Please identify the relevant federal entity category **(DESIGN NOTE: Multi select)**
Federal civilian executive branch (FCEB) - FISMA System (Yes/No)
Intelligence community (Yes/No)
Federal judicial branch (Yes/No)
Federal legislative branch (Yes/No)

DOD system, program, or platform (Yes/No)
[Op] + [RR] Is the system identified as part of the High Value Asset (HVA)[57] Program (Yes/No) **(DESIGN NOTE: Potential future NCISS question)**
[Op] + [RR] Is the impacted system designated as a National Security System[58] (Yes/No) **(DESIGN NOTE: Potential future NCISS question)**
{Conditional} **(DESIGN NOTE: Conditional to "Yes" selection to "B.1.a. Federal Civilian Executive Branch (FCEB) - FISMA System (Yes/No)". If Yes)**
[FISMA Req] Please provide the FISMA system name **(DESIGN NOTE: Pull from entry already entered in System list Q 65, and allow reporter to also identify as FISMA system and append additional attributes below.)**
[FISMA Req] Please select the type of FISMA system
General support system
Major application
Other
Please provide the system type **(DESIGN NOTE: Open text)**
[CUI] [FISMA Req] Contact information of the federal employee identified as the system owner
Name
First
Last
Phone number(s)
Unclassified
[Op]Classified
Email address(es)
Unclassified
[Op]Classified
Position or title
{Conditional}**(DESIGN NOTE: Conditional to "Yes" selection to C. High Value Asset (HVA) Program (Yes/No).) (DESIGN NOTE: Requirement to "connect" to the currently HVA databases as much as possible and technically capable with OCIO and Service Now.) (DESIGN NOTE: Potential future NCISS question; if Yes:)**
What is the HVA Identification Number? **(DESIGN NOTE: Per HVA program, this is the identification number to be able to connect with CISA's HVA database. The following questions may be able to be populated via HVA database but needs to be developed during design, if possible. If not possible, then the following questions should be asked of the reporter.)**
For each HVA listed, what services does it provide?
For each service, what communities does it support? **(DESIGN NOTE: Open text)**
Does this HVA have connections to other HVAs? (Yes/No)
(DESIGN NOTE: If Yes) Are these connections internal to the agency, external to the agency, or both? (Internal/External/Both)
(DESIGN NOTE: If Yes) Do you know what the other HVAs are? (Yes/No)
(DESIGN NOTE: If Yes) Please list the other HVA(s).
For each HVA listed, what services does it provide? **(DESIGN NOTE: Open text)**
For each service, what communities does it support? **(DESIGN NOTE: Open text)**
Do you have contact information for the other HVA(s)? (Yes/No)
[CUI] **(DESIGN NOTE: If Yes)**
Name
First
Last

[57] https://www.cisa.gov/resources-tools/programs/high-value-asset-program-management-office
[58] NSS is defined in law here: 40 USC 11103: Applicability to national security systems (house.gov) https://uscode.house.gov/view.xhtml?req=(title:40%20section:11103%20edition:prelim)%20OR%20(granuleid:USC-prelim-title40-section11103)&f=treesort&num=0&edition=prelim

Phone number(s)
Unclassified
[Op]Classified
Email address(es)
Unclassified
[Op]Classified
Position or title
Time zone

52. Incident Stage (A): Initial Access "Patient Zero" Details



{Conditional}[Op] + [RR] **(DESIGN NOTE: Executes if reporter has identified one or more TTPs observed above in the "Initial Access" category in any of the MITRE ATT&CK TTP matrices (example in "red box" to the right), this list is a "Dynamically created" list at time of question determined by which MITRE ATT&CK "Initial Access" TTPs were selected.)** You have observed and identified an "initial access" TTP[59] in this incident. Have you identified the initially affected endpoint, device, account, and/or application commonly referred to as "patient zero"? (Yes/No) **(DESIGN NOTE: If Yes, go to Q 65.)**
{Conditional}[Op] + [RR] **(DESIGN NOTE: Trigger this question if no MITRE ATT&CK TTPs were entered to identify any Initial Access TTPs and the narrative response has been parsed into discrete TTPs to create a list.)** Have you identified and initial access TTPs that you have attributed as the initial entry into your networks, commonly referred to as "patient zero"? (Yes /No) **(DESIGN NOTE: If Yes, go to Q 63.)**
{Conditional}[Op] + [RR] > [Triggered only if "Yes" from either Q63 or Q64] Please select from your reported initial access observed activity: TTP(s) and provide the technique used to gain the initial access to patient zero

(**DESIGN NOTE: Allow to select from previously entered Initial Access TTP list or the parsed narrative list if applicable first.)**
(DESIGN NOTE: If Yes) Was the "patient zero" also already entered with the rest of the impacted systems? (Yes/No)
(DESIGN NOTE: If Yes) Please select from your list of impacted systems the system(s) you believe to be "patient zero". **(DESIGN NOTE: Allow to select from previously entered impacted system (from question highlighted**

[59] Tactics, Techniques and Procedures (TTP)

in "red box" below) list of "table responses" and if not already entered, then allow for a similar table entry.

[C-15][RA] With respect to information systems you own and/or operate that are impacted by or involved in this incident: **(DESIGN NOTE: These set of questions repeat for every "instance" of Impacted Systems identified below.)**

A. [C-15][RA] Identify and describe the function of each individual (or group of similar) affected network(s), device(s), and/or Information System(s), specifically with respect to the category, system type, services provided, name, location and government customer communities supported:
   1. Category:
      a. Enterprise Networks or Systems[47]: Impacted [confirmed, suspected]
      b. Operational Technology[48] and Industrial Control Systems: Impacted [confirmed, suspected]
      c. Mobile Devices[49]: Impacted [confirmed, suspected]

   2. Systems Type **(DESIGN NOTE: Multi select then quantity entered) (DESIGN NOTE: Modify drop lists as accordingly per system category above, [e.g., if mobile device is selected, don't include options for "desktops" as an Endpoint device])**
      a. Endpoint Devices (non-Server devices)
         1. Authentication token or device
            i. Operating Systems (OS) **(DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option selected)**
               i. OS name(s)
               ii. OS version number(s)
               iii. Number impacted of each OS version
         2. Desktop
         3. Laptop

[C-15] **(DESIGN NOTE: If "No" or the system was not found in preexisting list then:)** If the system is not yet entered, please enter "patient zero" details now.
Select the initial access system category and type **(DESIGN NOTE: Follow same format as in previous Impacted System entries. Pull from the list already identified in question "Please Identify Impacted System". If already entered, allow reporter to select the system as "Patient Zero", otherwise allow reporter to enter in Patient Zero system details in same format.)**
When was the date/time of initial access in this incident?
Date and Time (yyyy-mm-dd HH:MM -<UTC offset>)

53. Incident Stage (A): Detailed Informational Impacts

(DESIGN NOTE: Execute this question if any impact is selected from the earlier Informational Impacts to Entity was selected (e.g., do NOT show if "No Impact" or "Unknown" were selected).)

[Op] + [RR] To the best of your knowledge, what is the current Informational Impact[33] of this incident?
A. No Impact
B. Minimal Impact
C. Significant Impact
D. Unrecoverable Impact
E. Unknown

[RC] Earlier in the form, you selected an informational impact[60] to your entity of **(DESIGN NOTE: Place selected choice of Informational Impact question here, e.g., "Significant Impact")**. We would like more details on your information impacts; can you please provide more details on any "suspected, but not confirmed" and/or "confirmed" known informational impact(s) from the incident?

(DESIGN NOTE: NCISS Variable = Informational Impact**)**

[60] **Informational Impact**: In addition to functional impact, incidents may also affect the confidentiality, integrity and availability of the information stored or processed by various systems. The information impact category is used to describe the type of information lost, compromised, or corrupted. (CISA National Incident Cyber Scoring System). CISA National Cyber Incident Scoring System (NCISS) | CISA

A. Please provide details on the "suspected" and/or "confirmed" informational impact(s) from this incident: **(DESIGN NOTE: (Multi select)**
   i. [] Suspected, but not yet confirmed
      1. Which of these information types do you suspect was impacted? **(DESIGN NOTE: Multi select)**

Classified material **(DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option selected) (DESIGN NOTE: if these follow-on questions are same per info type selected, give option to copy over the same responses)**
How was the suspected information impact discovered? (Select all that apply)
Some evidence of access but unclear evidence of exfiltration
Threat actor has provided inconclusive evidence of information impact (e.g., pictures of file directories)
Other inconclusive evidence of threat actor access/use of the information (please describe) **(DESIGN NOTE: Open text if selected)**
We were informed by an independent third party
Was the system where the information was located a critical system[61]? (Yes/No)
Communications (e.g., emails, instant messages)
Administrative credentials
User or other non-administrative credentials
Financial
Dissemination controlled
Legal
Proprietary
Other personal information
Defense information (as the information relates to unclassified cyber threat information/indicators (CTI), export controlled, operational security (OPSEC) and/or information)
Unclassified CTI
Export controlled information
OPSEC information

   ii. [] Confirmed
      1. **(DESIGN NOTE: If Yes)** What type of information impact? **(DESIGN NOTE: Select Privacy Data Breach and/or Other Data Compromise and/or Credential Compromise) (DESIGN NOTE: Multi select)**
         a. [ ] Privacy data breach **(DESIGN NOTE: If Privacy data breach, then ask following) (DESIGN NOTE: Multi select)**
            1. What type of information was impacted? **(DESIGN NOTE: Multi select)**

Financial **(DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option selected)**
How was the information loss identified? (Select all that apply)
The information was seen outside the authorized system (e.g., darkweb, leaksite, etc.) **(DESIGN NOTE: Flagged as exploited)**
The information was seen being exfiltrated from the authorized system and/or network **(DESIGN NOTE: Flagged as loss)**
We were informed by an independent third party **(DESIGN NOTE: Flagged as loss)**
Other evidence of threat actor access/use of the information (please describe) **(Design Note: Open Text if selected)**
Was the system where the information was located a critical system? (Yes/No)
Dissemination Controlled
Legal

[61] **Critical System/Services/Property:** Specific entity [system/service/property] that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation [or organization, business, entity] to continue to function effectively; [a system/service/property of great] importance to a mission or function, or continuity of operations. *[derived from "critical asset" page 135-136 and critically page 139 of https://www.dhs.gov/publication/dhs-lexicon*

Proprietary
Other personal information

b. [ ] Other data compromise **(DESIGN NOTE: If Other data compromise, then ask the following)**
   1. What type of information was impacted? **(DESIGN NOTE: Multi select)**

Communications **(DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option selected)**
How was the information loss identified
The information was seen outside the authorized system. (e.g., darkweb, leaksite, etc.) **(DESIGN NOTE: Flagged as exploited)**
The information was seen being exfiltrated from the authorized system and/or network **(DESIGN NOTE: Flagged as loss)**
We were informed by and independent third party **(DESIGN NOTE: Flagged as loss)**
Other evidence of threat actor access/use of the information (please describe) **(Design Note: Open Text if selected)**
Was the system where this information was located a critical system? (Yes/No)

i. Dissemination controlled
   i. Proprietary
ii. Classified
iii. Defense information (as the information relates to unclassified cyber threat information/indicators (CTI), export controlled, OPSEC and/or information)
   i. CTI
   ii. Export controlled information
   iii. OPSEC information

c. [ ] Credential compromise **(DESIGN NOTE: If credential compromise, then as the following)**
   a. What types of credentials were compromised? **(DESIGN NOTE: Multi select)**
      i. User or other non-administrative credentials **(DESIGN NOTE: 1.i.,ii.,iii.,iv and 2., repeated for each option selected)**
         1. How did you or others identify the compromise of the credentials? (Select all that apply)

The information was seen outside the authorized system (e.g., darkweb, leaksite, etc.) **(DESIGN NOTE: Flagged as exploited)**
The information was seen being exfiltrated from the authorized system and/or network **(DESIGN NOTE: Flagged as loss)**
We were informed by an independent third party **(DESIGN NOTE: Flagged as loss)**
Other evidence of threat actor access/use of the information (please describe) **(DESIGN NOTE: Open Text if selected)**

         2. Was the system where this information was located a critical system? (Yes/No)
      ii. Administrative credentials
         1. How was the compromise of the credentials identified? **(DESIGN NOTE: Select all that apply)**
            A. The information was seen outside the authorized system. (e.g., darkweb, leaksite, etc.) **(DESIGN NOTE: Flagged as exploited)**

B. The information was seen being exfiltrated from the authorized system and/or network **(DESIGN NOTE: Flagged as loss)**

C. We were informed by an independent third party **(DESIGN NOTE: Flagged as loss)**

D. Other evidence of threat actor access/use of the information (please describe) **(DESIGN NOTE: Open Text if selected)**

2. Was this credential on or did it have access to a critical system? (Yes/No)

54. Incident Stage (A): Breach Details

(DESIGN NOTE: Executes if incident is flagged as a Breach Incident in "Breach Severity Assessment" earlier as indicated in response to questions flagged in "red box" below:)

Breach[25] Severity Impacts

[Op] + [FISMA Req] At this time, has the incident resulted in any confirmed unauthorized access to personally identifiable information? (Yes/No) **(DESIGN NOTE: If Yes, flag as Breach Incident and include Incident Stage (A): Breach Details. Show follow-on short questions "access due" and "accessed by" only if "Yes".)**

A. Was the access due to (select all that apply):
   1. Loss of control
   2. Compromise
   3. Unauthorized disclosure
   4. Unauthorized acquisition

B. Was the information accessed by (select all that apply):
   1. A person other than an authorized user
   2. An authorized user who accessed the record(s) for an other-than-authorized purpose

{Conditional} [Op] + [FISMA Req] **(DESIGN NOTE: Do not ask this question if the "Confirmed Unauthorized Access" question yields a positive selection response. Only ask if previous response to "confirmed" = "No")** At this time, has the incident resulted in any potential unauthorized access to personally identifiable information? (Yes/No) **(DESIGN NOTE: If Yes, flag as Breach Incident and include Incident Stage (A): Breach Details. Show follow-on short questions "access due" and "accessed by" only if "Yes".)**

A. Was the potential unauthorized access due to: (select all that apply)
   1. Loss of control
   2. Compromise
   3. Unauthorized disclosure
   4. Unauthorized acquisition

B. Was the information potentially accessed by: (select all that apply)
   1. A person other than an authorized user
   2. An authorized user who accessed the information for an other-than-authorized purpose

[Op] + [FISMA Req] Earlier in this form, you provided the following description of this incident: **(DESIGN NOTE: Pull forward the information entered by reporter earlier as flagged in the "red box" below:)**

[RA] Provide a high-level summary of the incident. **(DESIGN NOTE: Open Text) (DISPLAY NOTE: Requests for more details will occur later in this report. Please provide a short "Executive Summary" of the incident with a narrative of the incident detection. Consider including a description of any unauthorized access (including whether the incident involved an unattributed cyber intrusion); identification of any informational impacts or information compromise; any network location where activity was observed; and a high-level description of the impacted system(s) (e.g., "email servers, a network firewall, and a web server").)**

You have also previously indicated there was actual or potential unauthorized access to personally identifiable information (PII). Please add any available additional context on the PII that was impacted. However, DO NOT include samples of actual PII in this response.

[FISMA Req] Did this incident involve a cyber- or non-cyber-related breach of PII? **(DESIGN NOTE: Single-select)**

Cyber-related
Non-cyber related (e.g., personnel information with PII found in a public dumpster)
Both

[FISMA Req] If you have any additional details regarding what has been observed or identified with respect to the PII breach, please describe that here. However, DO NOT include samples of actual PII in this response. **(DESIGN NOTE: Open text)**

55. Impacted Individuals:

[FISMA Req] How many individuals' PII was impacted[62]?

[62] **Impact**: is defined by CDM as "the loss of confidentiality, integrity, or availability that could be expected to have an adverse effect on organizational operations or organizational assets or individuals (CDM Glossary of Terms).

[FISMA Req] Were affected individuals notified? (Yes/No/Pending)
(DESIGN NOTE: If Yes or Pending) How were (or will the) individuals (be) notified? (Select all applicable)
Email
How many individuals were (or will be) notified using this method?
Short message service (SMS)
How many individuals were (or will be) notified using this method?
Verbal
How many individuals were (or will be) notified using this method?
Parcel
How many individuals were (or will be) notified using this method?
Other (Please list the method that was or will be used)
How many individuals were notified using this method?
[CUI] [FISMA Req] Were mitigation services in the form of monitoring, insurances and/or counseling provided or offered to affected individuals? (Yes/No)
(DESIGN NOTE: If Yes) Which mitigation services have you made available to impacted individuals? (Please select all that apply)**:**
Identity monitoring
Credit monitoring
Identity theft insurance
Full-service identity counseling and remediation services
[CUI] Other (describe)

56. PII Accessed and/or Impacted:

[FISMA Req] For each type of PII, provide how many records instances of a PII category or type were accessed, potentially accessed, or otherwise impacted? **(DISPLAY NOTE: Use approximate counts if final counts are not available) (DESIGN NOTE: Multi select for each PII "category" (e.g.., Identifying numbers, Biographical Information, etc.) with the appropriate "accessed or impacted flags".)**
Personally Identifying Numbers **(DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated for each response selected) (DESIGN NOTE: Allow for reporters' ability to scan through this whole list or provide the ability to search. Possible recommendation is to order these based on how common they are (e.g., agency specific numbers should be later, but things like passport number, payment card number, bank account numbers should be near the top.)**
Full social security number
Provide count
Is this count known or approximate? (Known/Approximate)
Did potential or confirmed access occur? (Potential/Confirmed)
Truncated or partial social security number
Driver's license number
License plate number
Drug Enforcement Administration (DEA) registration number
File/case identification (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)
Other (please identify)
Biographical Information **(DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated for each response selected.)**
Full name (First, Last, including nicknames)
Provide count
Is this count known or approximate? (Known/Approximate)
Did potential or confirmed access occur? (Potential/Confirmed)
Gender
Race
Date of birth (day, month, year)
Ethnicity
Nationality
Country of birth
City or county of birth
State 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, but not including account or payment card numbers)
Business financial information (including loan information, but not including account or payment card numbers)
Alias (i.e., username or screenname)
Education information
Resume or curriculum vitae **(DISPLAY NOTE: If these documents include additional types of PII, e.g., address or SSN, please indicate those fields separately.)**
Professional/personal references **(DISPLAY NOTE: If these documents include additional types of PII, e.g., address or SSN, please indicate those fields separately.)**
Biometrics, Distinguishing Features, and Characteristics **(DESIGN NOTE" Multi select and for sub questions "a., b., c.", repeated for each response selected.)**

Fingerprints
Provide count
Is this count known or approximate? (Known/Approximate)
Did potential or confirmed access occur? (Potential/Confirmed)
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/Health and Emergency Information **(DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated for each response selected.)**
Physical medical/health information
Provide count
Is this count known or approximate? (Known/Approximate)
Did potential or confirmed access occur? (Potential/Confirmed)
Mental health information
Disability information
Workers' compensation information
Patient ID number
Emergency contact information
Device Information **(DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated for each response selected.)**
Device settings or preferences (e.g., security level, sharing options, ringtones)
Provide count
Is this count known or approximate? (Known/Approximate)
Did potential or confirmed access occur? (Potential/Confirmed)
Cell tower records (i.e., logs, user location, time, etc.)
Network communications data
Other Specific Information or File Types **(DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated for each response selected.)**
Taxpayer information/Tax return information
Provide count
Is this count known or approximate? (Known/Approximate)
Did potential or confirmed access occur? (Potential/Confirmed)
Law enforcement information
Security clearance/background check information
Civil/criminal history information/police record
Academic and professional background information
Health information
Case files
Personnel files
Credit history information
Other
Please provide the other specific information or file type(s)

57. Incident Stage (A): Security Control(s) [Contributing to Incident]

[Op] + [RR but **NOT FISMA or FedRAMP reporting**] Please review the "Protect" section of the CISA Cross-Sector Cybersecurity Performance Goals (CPGs).[63] To the best of your knowledge, did the implementation (or lack thereof), misconfiguration, or failure of a security control (as described in CISA's Protect CPGs)[64] lead to, contribute to, or otherwise factor into your incident? (Yes/No)

A. Yes
   i. **(DESIGN NOTE: If Yes)** Select all that apply [ ] non-implementation [ ] misconfiguration and/or [ ] failure of the security control
B. No
C. Unknown **(DESIGN NOTE: If the person selects "Unknown", then DISPLAY NOTE: When and if, during your investigation, you discover knowledge about security controls contributing to the incident, please return to this question and share any details you can about security controls where the implementation (or lack thereof), improper configuration, or other aspect of the control led to, contributed to, or otherwise factored into the incident.)**

{Conditional if Q 79 = Yes} [Op] + [RC] Select the applicable control(s) from the CISA Cybersecurity Performance Goals, "Protect" section[65].

A. Select from **[DESIGN NOTE: See Appendix 2 for answer options, multi choice select) (DESIGN NOTE: Repeat for each CPG Protect Control selected)**

(DISPLAY NOTE: Select one) Was the [ ] failure, [ ] misconfiguration, or [ ]non-implementation of the control due to a published CVE[66](s)?

Yes **(DESIGN Note: The following "CVE" questions are conditional only if the reporter selected "YES" to security controls factoring into the incident)**

What is the CVE(s)? **(DESIGN NOTE: Allow for more than one entry and look up the CVE in KEV and display to reporter)**

(DESIGN NOTE: Multi select for Failed, Misconfigured, and Not implemented) (repeat for each CVE identified)

No

Unknown

Do one or more of the observed TTPs reported earlier in this report relate to this selected security control? (Yes/No)

(DESIGN NOTE: If Yes) Please select from your reported observed TTPs those that are attributed to this security control **(DESIGN NOTE: Display all TTPs [MITRE ATT&CK and general] that have been reported and allow user to select one or more TTPs and associate with this/these security control(s).)**

Please provide any additional information regarding how security control implementation, failure, misconfiguration, or non-implementation played a role in this incident **(DESIGN NOTE: Open text) (DISPLAY NOTE: This includes not only any additional information regarding how failure, misconfiguration, or non-implementation of a control may have contributed to an incident, but also information regarding any controls that were also effective in mitigating or detecting the incident, and/or controls that worked and forced the threat actor to pivot to something more complex, etc.)**

[**FISMA or FedRAMP reporting only**] **(DISPLAY NOTE: CISA understands the NIST SP 800-53 and NIST SP 800-171 are primary sources to follow when establishing and setting various system controls under FISMA and FedRAMP requirements. CISA also acknowledges others outside FISMA and FedRAMP may not be as familiar with these publications. Therefore, CISA has implemented two paths for identifying security controls that have contributed to the incident. For FISMA and/or FedRAMP reporting the NIST publications are available to reference. For all other reporting, the "Protect" section of the CISA Cross-**

[63] Cross-Sector Cybersecurity Performance Goals | CISA (https://www.cisa.gov/cross-sector-cybersecurity-performance-goals)

[64] See Appendix 2

[65] See Appendix 2

[66] CVE is a program that identifies, defines, and catalogs publicly disclosed cybersecurity vulnerabilities. https://cve.mitre.org/

Sector Cybersecurity Performance Goals (CPGs)[67] will be referenced.) To the best of your knowledge, did the implementation (or lack thereof), misconfiguration, or failure of a security control (as described in NIST SP 800-53) lead to, contribute to, or otherwise factor into your incident? (Yes/No)

A. Yes
    i. **(DESIGN NOTE: If Yes)** Select all that apply [ ] non-implementation [ ] misconfiguration and/or [ ] failure of the security control
B. No
C. Unknown **(DESIGN NOTE: If the person selects "Unknown", then DISPLAY NOTE: When and if, during your investigation you discover knowledge about security controls contributing to the incident, please return to this question and share any details you can about security controls where the implementation (or lack thereof), improper configuration, or other aspect of the control led to, contributed to, or otherwise factored into the incident.)**

{Conditional if Q 81 = Yes} [**FISMA and FedRAMP only**] **(DISPLAY NOTE: To enhance trends and analysis of security controls between incidents, establishing a common reference is a sound approach. Therefore, CISA has associated the CISA CPGs with a subset of NIST SP 800-53 controls (NIST SP 800-171 is in development). You will have an opportunity to select this subset first if applicable, then can select from the remaining NIST SP 800-53 set of controls if necessary.)** Select the applicable control(s) from NIST SP 800-53 (CPG preferred list first), then if applicable select from the remaining controls.

A. Select from **(DESIGN NOTE: provide NIST SP 800-53 subset list per Appendix 2 CPG to NIST SP 800-53 mapping as first dropdown list, then provide another dropdown list identifying remaining NIST SP 800-53 controls) (DESIGN NOTE: Repeat for each control selected, multi choice select)**

(DISPLAY NOTE: Select one) Was the [ ] failure, [ ] misconfiguration, or [ ]non-implementation of the control due to a published CVE[68](s)?

Yes **(DESIGN Note: The following "CVE" questions are conditional only if the reporter selected "YES" to security controls factoring into the incident)**

What was the CVE(s)? **(DESIGN NOTE: Allow for more than one entry and look up the CVE in KEV and display to reporter)**

(DESIGN NOTE: Multi select for Failed, Misconfigured, and Not implemented) (repeat for each CVE identified)

No

Unknown

Does one or more of the observed TTPs reported earlier in this report relate to this selected security control? (Yes/No)

(DESIGN NOTE: If Yes) Please select from your reported observed TTPs the one(s) that are attributed to this security control **(DESIGN NOTE: Display all TTPs [MITRE ATT&CK and general] that have been reported and allow user to select one or more TTPs and associate with this/these security control(s).)**

Please provide any additional information regarding how security control implementation, failure, misconfiguration, or non-implementation played a role in this incident **(DESIGN NOTE: Open text) (DISPLAY NOTE: This includes not only any additional information regarding how failure, misconfiguration, or non-implementation of a control may have contributed to an incident, but also information regarding any controls that were also effective in mitigating or detecting the incident, and/or controls that worked and forced the threat actor to pivot to something more complex, etc.)**

[67] Cross-Sector Cybersecurity Performance Goals | CISA (https://www.cisa.gov/cross-sector-cybersecurity-performance-goals)

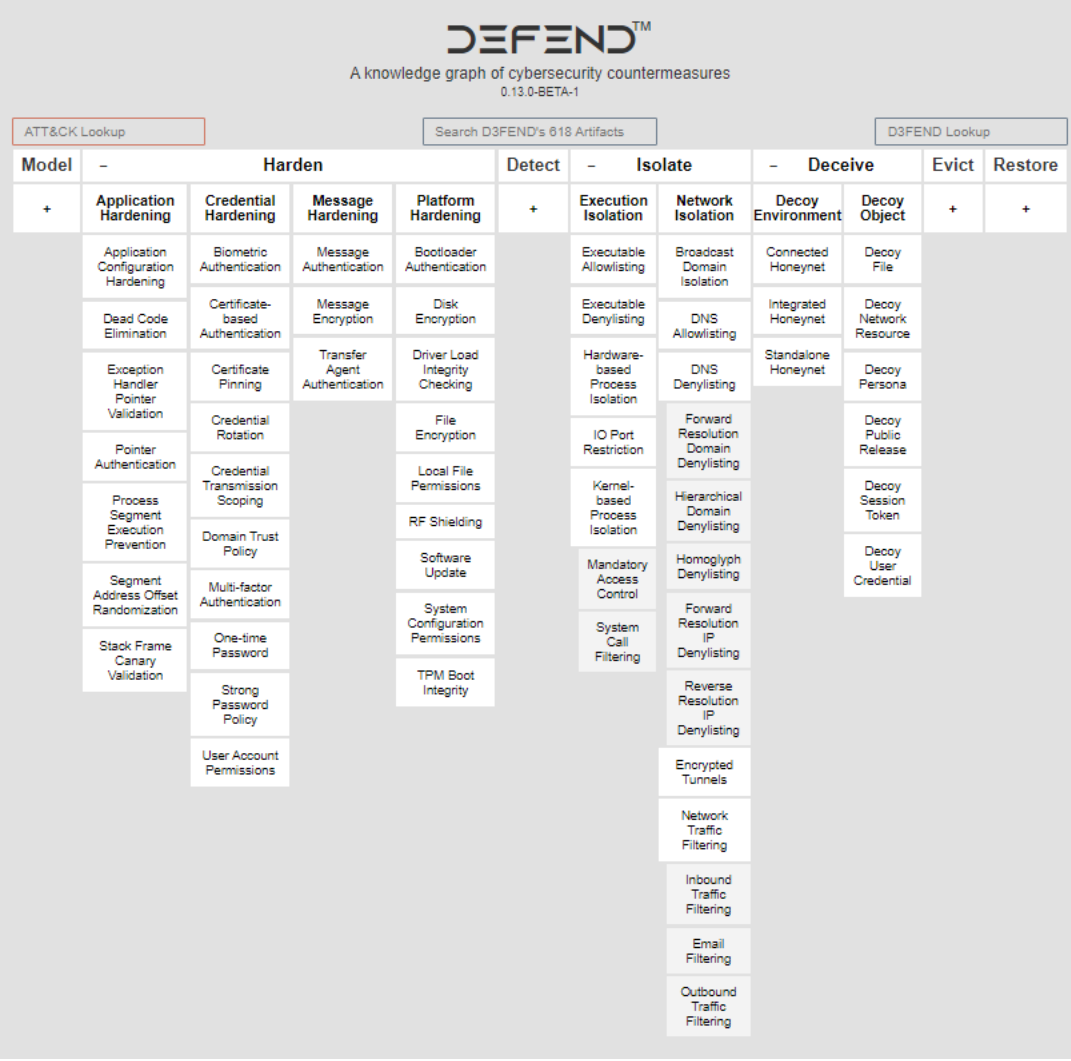
[68] CVE is a program that identifies, defines, and catalogs publicly disclosed cybersecurity vulnerabilities. https://cve.mitre.org/

Containment Stage [69](C)
[Op] + [FISMA Req] Have you begun the containment stage? (Yes/No/Unsure) (Note: This stage involves taking steps to prevent the incident from spreading further.)
(DESIGN NOTE: If Yes) Provide the date and time (yyyy-mm-dd HH:MM -<UTC offset>) containment activities began
Provide an overview of your containment strategy
If implementation of the containment strategy is complete, was the containment strategy successful? (Y/N)
(DESIGN NOTE: If No) Provide details on how your strategy is changing **(DESIGN NOTE: Open text)**
[CUI] {Conditional} [Op] + FISMA Req] What specific containment action(s) have been taken? **(DESIGN NOTE: Can be more than one, include options to add)**
Description **(DESIGN NOTE: Open text)**
Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
Has this action been completed? (Yes/No)
(DESIGN NOTE: If Yes) Was this action successful? (Yes/No)
(DESIGN NOTE: If No) Can you identify why it wasn't successful? **(DESIGN NOTE: Open text)**
[CUI] **(DESIGN NOTE: If No)** Provide details on how your containment action is changing **(DESIGN NOTE: Open text)**
[RC] Have you completed containment? (Y/N)

58. Incident Stage (C): Countermeasures – Containment

[Op] + [FISMA Req] As explained earlier, the MITRE D3FEND matrix categorizes countermeasures into multiple categories. Containment actions are identified in the "harden," "isolate," and "deceive" categories. Please select the containment actions you have taken from among these categories**. (DESIGN NOTE: Display of this section to be similar to that of MITRE D3FEND site) (DESIGN NOTE: See** https://d3fend.mitre.org/ **for MITRE D3FEND list. The recommendation is to display similar to the actual MITRE D3FEND matrix for a visual navigation.)**
(Select all that apply)
Select applicable "containment" counter measures from the MITRE D3FEND list:

[69] Containment Stage – Stage of the incident life cycle that employs activities before an "incident overwhelms resources or increases damage. Containment provides time for developing a tailored remediation strategy" and can involve many different approaches based on the known severity of the incident as determined during the Analysis Stage "(e.g., shut down a system, disconnect it from a network, disable certain functions)." [derived from pg 35 of NIST 800-61 r2]



[Op] We are unable to use MITRE D3FEND to identify "containment" countermeasures used during this incident, or our organization leveraged a "containment" countermeasure not listed or that is currently unidentified in MITRE D3FEND

Did you employ a containment technique that potentially fit within an existing "MITRE D3FEND tactic" but was not listed? (Yes/No) **(DISPLAY NOTE: The top-line categories associated with containment are "harden", "isolate", or "deceive". These are considered the "tactics".)**

(DESIGN NOTE: If Yes)

Which tactic did your containment action fall under?

Harden

Which base technique did your action fall under?

Application hardening

Credential hardening

Message hardening

Platform hardening

Isolate

Which base technique did your action fall under?

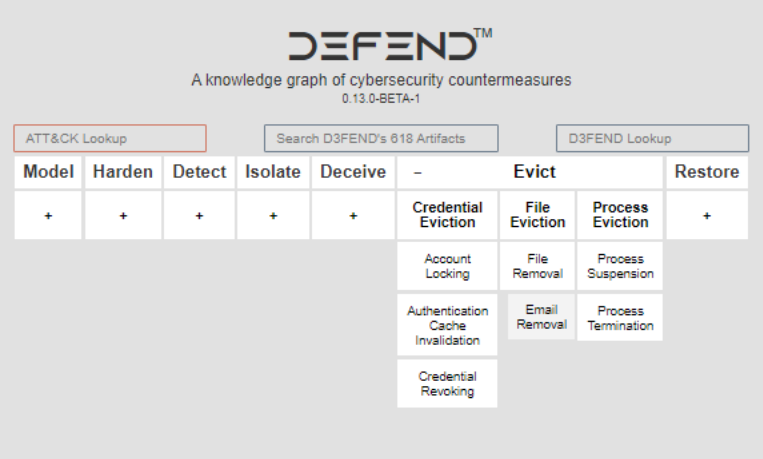
Execution isolation

Network isolation
Deceive
Which base technique did your action fall under?
Decoy environment
Decoy object
Description **(DESIGN NOTE: Open text)**
(DESIGN NOTE: If No) If unable to use MITRE D3FEND to identify "containment" countermeasures used during this incident and cannot bucket the countermeasure into an existing MITRE D3FEND category, please provide a description and details of the countermeasures you have employed **(DESIGN NOTE: Open text)**
Unknown
None
[Op] Please provide any additional context for the "containment" countermeasures you have taken **(DESIGN NOTE: Open text)**
Eradication Stage [70](E)
[CUI] [Op] + [FISMA Req] Have you begun the eradication stage? (Yes/No/Unsure)
[If Yes] Provide the date and time (yyyy-mm-dd HH:MM -<UTC offset>) eradication activities began.
[CUI] {Conditional} [Op] + [FISMA Req] Provide an overview of your eradication strategy **(DESIGN NOTE: Open text)**
{Conditional} [Op] + [FISMA Req] Have you completed the eradication activities? (Yes/No)
(DESIGN NOTE: If Yes) Please provide date and time (yyyy-mm-dd HH:MM -<UTC offset>)
(DESIGN NOTE: If No) Is the implementation of your eradication strategy complete? (Y/N)
(DESIGN NOTE: If No) Was the eradication strategy successful? (Y/N)
(DESIGN NOTE: If No) Provide details on how your eradication strategy is changing **(DESIGN NOTE: Open text)**
(DESIGN NOTE: If No) What specific eradication action(s) have been taken? **(DESIGN NOTE: Can be more than 1, include options to add)**
Description **(DESIGN NOTE: Open text)**
Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
Has this action been completed? (Yes/No)
(DESIGN NOTE: If Yes) Was this action successful? (Yes/No)
(DESIGN NOTE: If No) Can you identify why it wasn't successful?
(DESIGN NOTE: If No) Provide details on how your eradication action is changing.

59. Incident Stage (E): Countermeasures – Eradication

[Op] + [FISMA Req] As noted earlier, the MITRE D3FEND matrix categorizes countermeasures into multiple categories. Eradication actions are identified in MITRE's D3FEND matrix in the "evict" category. Please select the eviction actions you have taken from this category **(DESIGN NOTE: Display of this section to be similar to that of MITRE D3FEND site) (DESIGN NOTE: See** https://d3fend.mitre.org/ **for MITRE D3FEND list. The recommendation is to display similar to the actual MITRE D3FEND matrix for a visual navigation)** Select all that apply.
Select applicable "evict" counter measures from the MITRE D3FEND list:

[70] Eradication Stage: Stage of the incident life cycle the follows one or more containment activities and results of further analysis that "may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated [and remove any remnants of invalid computer code, invalid system accounts and other threat actor influenced system configurations to eliminate the threat.] For some incidents, eradication is either not necessary or is performed during recovery (e.g., files are restored from valid backups)." [derived from pg. 37 of NIST 800-61 r2]



[Op] We are unable to use MITRE D3FEND to identify eradication counter measures used during this incident, or our organization leveraged an eradication counter measure not listed or that is currently unidentified in MITRE D3FEND.

Did you employ a eradication technique that potentially fit within an existing "MITRE D3FEND tactic" but was not listed? (Yes/No) **(DISPLAY NOTE: The top-line category associated with eradication is: "evict". This is considered the "tactics")**

(DESIGN NOTE: If Yes) Which evict technique did you action fall under?

Credential eviction

Description

File eviction

Description

Process eviction

Description

Please provide a description and details of the counter measures you have employed **(DESIGN NOTE: Open text)**

(DESIGN NOTE: If No) If unable to use MITRE D3FEND to identify "eradication" counter measures used during this incident and cannot bucket the counter measure into an existing MITRE D3FEND category, please provide a description and details of the counter measures you have employed **(DESIGN NOTE: Open text)**

Unknown

None

[CUI] {Conditional} [Op] + [FISMA Req] Please provide any additional context for the "eradication" actions you have taken **(DESIGN NOTE: Open text)**

Recovery Stage [71](R)

[CUI] [Op] + [FISMA Req] Have you begun the recovery stage? (Yes/No/Unsure) **(DISPLAY NOTE: In the recovery stage, the focus is on restoring affected systems and services to normal operation.)**

[RC] **(DESIGN NOTE: If Yes)**

Provide the date and time (yyyy-mm-dd HH:MM -<UTC>) Please enter the organization's estimated recovery date and time

Date and time (yyyy-mm-dd HH:MM -<UTC offset>)

[Op] + FISMA Req] Describe your recovery strategy **(DESIGN NOTE: open text)**

[Op] + [FISMA Req] Have you completed the recovery stage and "accepted" normal operations resumed? (Yes, No)?

(DESIGN NOTE: If Yes) Please provide the Date and Time (yyyy-mm-dd HH:MM -<UTC offset>)

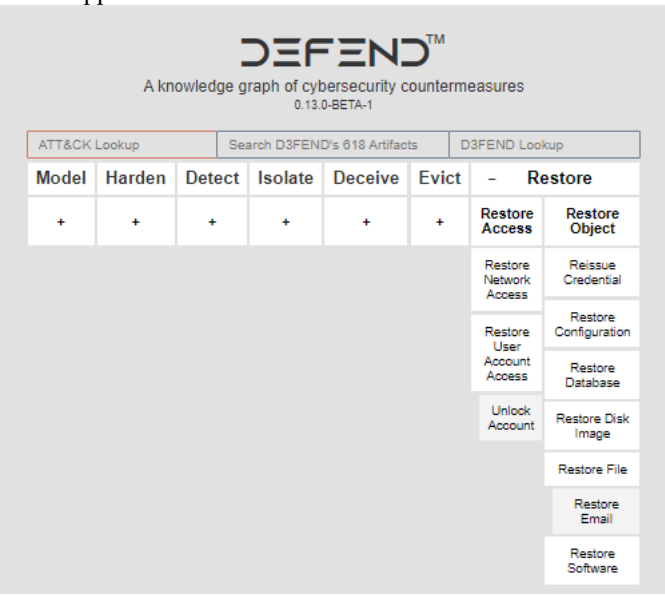
[71] Recovery Stage - Stage in the Incident Life cycle that provides "restoration of critical information technology systems and services" to normal [or newly accepted] operations and within an accepted (by the owning entity) time period. "Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists)." [derived from "intermediate recovery". page 347 of https://www.dhs.gov/publication/dhs-lexicon and pg. 37 of NIST 800-61 r2]

Was the recovery strategy successful? (Yes/No)
(DESIGN NOTE: If No)
Did you modify your strategy after you began recovery? (Yes/No)
[CUI] **(DESIGN NOTE: If Yes)** Why did you modify the strategy? **(DESIGN NOTE: Open text)**

(DESIGN NOTE: NCISS Variable = Recoverability Impact)
[Op] + [RR] Estimate the scope of resources needed to recover from the incident (recoverability).
Regular **(DISPLAY NOTE: (Provide hover-over) Time to recover is predictable with existing resources.)**
Supplemented **(DISPLAY NOTE: (Provide hover-over) Time to recover is predictable with additional resources.)**
Extended **(DISPLAY NOTE: (Provide hover-over) Time to recover is unpredictable; additional resources and outside help are needed.)**
Not recoverable **(DISPLAY NOTE: (Provide hover-over) Recovery from the incident is not possible (i.e., sensitive data exfiltrated and posted publicly).)**

60. Incident Stage (R): Recovery Actions

[Op] + [FISMA Req] As noted earlier, the MITRE D3FEND matrix categorizes countermeasures into multiple categories. Recovery activities are identified in MITRE's D3FEND matrix in the "restore" category. Please select the recovery actions you have taken from this category. **(DESIGN NOTE: Display of this section to be similar to that of MITRE D3FEND site) (DESIGN NOTE: See https://d3fend.mitre.org/ for MITRE D3FEND list. The recommendation is to display similar to the actual MITRE D3FEND matrix for a visual navigation.)** Select all that apply.
Select applicable "restore" measures from the MITRE D3FEND list:



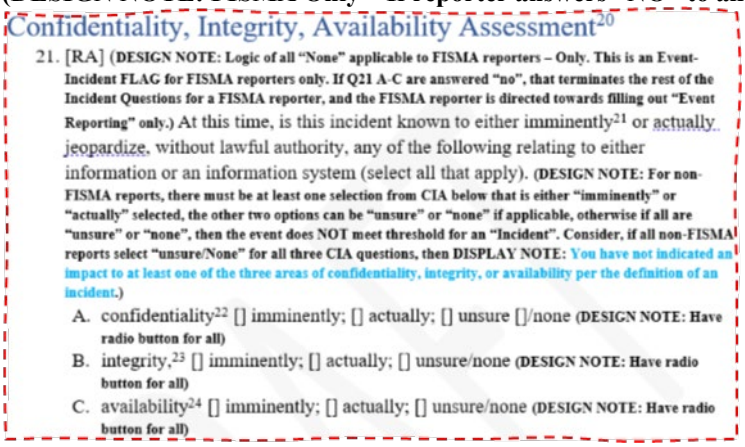
[Op] We are unable to use MITRE D3FEND to identify "recovery" countermeasures used during this incident, or our organization leveraged a "recovery" counter measure not listed or that is currently unidentified in MITRE D3FEND.
Did you employ a recovery technique that potentially fit within an existing "MITRE D3FEND tactic" but was not listed? (Yes/No) **(DISPLAY NOTE: The top-line category associated with "recovery" is: "restore." This is considered the "tactic"),**
(DESIGN NOTE: If Yes) Which restore technique did your action(s) fall under:
Restore access
Description
Restore object

Description
(DESIGN NOTE: If No) If unable to use MITRE D3FEND to identify "recovery" countermeasures used during this incident, and you cannot bucket your counter measure into an existing MITRE D3FEND category, please provide a description and details of the counter measures you have employed. **(DESIGN NOTE: Open text)**
Unknown
None
[Op] + [FISMA Req] Please describe any additional recovery steps you have taken (e.g., additional external outreach and/or support, update any relevant policies, procedures, and plans, such as incident response plans, continuity of business plans, disaster recovery plans, system back-up and restore plans, business exercise plans) **(DESIGN NOTE: Open text)**

Post-Incident Stage (P-I)
[Op] + [FISMA Req] Has the incident concluded? (Yes/No)
(DESIGN NOTE: If Yes) Provide your post incident report/details
[Op] + [FISMA Req] If available, submit any post incident or after-action reports related to this incident **(Submit your organization's post incident report (WITH AN UPLOAD FILE OPTION HERE.) (DISPLAY NOTE: For Federal civilian executive branch agencies, this is in line with CISA's Incident Playbook to allow CISA to "validate organization's response".)**[72]
[Op] + [FISMA Req] Looking back on your incident response, was there information that, had you received it or learned it sooner, would have led to a more streamlined, quicker, and/or more effective incident response? If yes, identify the incident response stage where you would have preferred to receive this information. **(DESIGN NOTE: Multi select; based on NIST 800-61 r2, the major phases of an incident life cycle.)**
Identification and detection
Which organization could have provided the information? **(DESIGN NOTE: Repeated for each stage selected.)**
Analysis
Containment
Eradication
Recovery
Post-incident
[Op] + [FISMA Req] Has the impacted organization performed a review of the incident and incident response to identify lessons learned? (Y/N)
(DESIGN NOTE: If Yes) Please describe the identified lessons learned in the areas of:
Incident handling processes
Mean time to effective analysis
Mean time to detection
Mean time to response
Mean time to defense
Mean time to reporting
Other
[Op] + [FISMA Req] Based on your experience in this incident, please provide recommendations on how CISA can improve the support it provides
What could CISA do differently in future incidents? **(DESIGN NOTE: Open text)**
Are there indicators of compromise or relevant detection mechanisms you have not provided previously in this report and believe can enable detection of similar incidents in the future? **(DESIGN NOTE: Open text)**
What additional tools or resources would you need to detect, analyze, and mitigate future incidents? **(DESIGN NOTE: Open text)**

[72] Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems: Publication: November 2021

Event Reporting (Below Incident Thresholds) (FISMA – Only)
(DESIGN NOTE: FISMA Only – If reporter answers "NO" to all CIA Impact Assessments)



Confidentiality, Integrity, Availability Assessment[20]

21. [RA] (**DESIGN NOTE: Logic of all "None" applicable to FISMA reporters – Only. This is an Event-Incident FLAG for FISMA reporters only. If Q21 A-C are answered "no", that terminates the rest of the Incident Questions for a FISMA reporter, and the FISMA reporter is directed towards filling out "Event Reporting" only.**) At this time, is this incident known to either imminently[21] or actually jeopardize, without lawful authority, any of the following relating to either information or an information system (select all that apply). (**DESIGN NOTE: For non-FISMA reports, there must be at least one selection from CIA below that is either "imminently" or "actually" selected, the other two options can be "unsure" or "none" if applicable, otherwise if all are "unsure" or "none", then the event does NOT meet threshold for an "Incident". Consider, if all non-FISMA reports select "unsure/None" for all three CIA questions, then DISPLAY NOTE: You have not indicated an impact to at least one of the three areas of confidentiality, integrity, or availability per the definition of an incident.**)
    A. confidentiality[22] [] imminently; [] actually; [] unsure []/none (**DESIGN NOTE: Have radio button for all**)
    B. integrity,[23] [] imminently; [] actually; [] unsure/none (**DESIGN NOTE: Have radio button for all**)
    C. availability[24] [] imminently; [] actually; [] unsure/none (**DESIGN NOTE: Have radio button for all**)

[FISMA Req] Has this activity already been reported? (Yes/No)

1. **(DESIGN NOTE: If Yes)** Provide
    1. Incident report form submission number.
    2. CISA incident tracking number.

[CUI] [FISMA Req] Describe the scope of impacted systems and provide a high-level summary of the event activity. **(DESIGN NOTE: Narrative of the event detection)**
[FISMA Req] When did you first detect the activity?

A. Date and time (yyyy-mm-dd HH:MM -<UTC offset>)

[FISMA Req] When did you declare an event?

A. Date and time (yyyy-mm-dd HH:MM -<UTC offset>)

[FISMA Req] Please provide any additional information relevant to the event **(DESIGN NOTE: Open text)**
[FISMA Req] Has the entity covered by this event resolved the consequences for the event?
(DESIGN NOTE: If Yes) Provide the date and time when the event was resolved
Recovered as of date/time (yyyy-mm-dd HH:MM -<UTC offset>)
[FISMA Req] [FISMA Req] Please describe any additional steps you have taken to resolve the event (e.g., additional external outreach and/or support, update any relevant policies, procedures, and plans, such as incident response plans, continuity of business plans, disaster recovery plans, system back-up and restore plans, business exercise plans) **(DESIGN NOTE: Open text)**

Data Marking Stage

61. Cybersecurity Information Sharing Act of 2015 Acknowledgement

(DESIGN NOTE: Only Show for Non-Federal Voluntary Reporters [i.e., Voluntary Report] or Non-Federal Non-Voluntary Reporters [e.g., TSA], not to be shown for FISMA reporters)
[Op] + [Not Applicable to FISMA Reporting] To the extent not already indicated using the data markings, do your responses to any of the questions above constitute cyber threat indicator(s) or defensive measure(s) submitted under the Cybersecurity Information Sharing Act of 2015 that the submitter is requesting be treated as *commercial, financial, and proprietary*? (Yes/No)
(DESIGN NOTE: If Yes) Select question numbers **(DESIGN NOTE: Provide drop-down, multi select).**

62. Overall Report Data Markings:

[CUI] [Op] + [RR] The most restrictive marking that has been reported in this incident is X.[73] Is this a valid marking for the entire incident? (Yes/No)
(DESIGN NOTE: If Yes) Then the incident marking is X.[74]
(DESIGN NOTE: If No) User to enter new marking for the entire incident

[73] The default data marking presented here
[74] The accepted default data marking here

(DESIGN NOTE: See Appendix 1 for question options[75])

End of Incident Reporting Questions

Appendix 1: Data Marking

63. Data Marking Options

Specific data marking options are as follows

1. [C-15] Cybersecurity Information Sharing Act of 2015 *commercial, financial, and proprietary*[76]
2. [CUI] Controlled unclassified information (CUI)[77]

Appendix 2: CISA Cybersecurity Performance Goals[78] (Protect) & NIST SP 800-53 References

64. Protect CISA CPGs & NIST SP 800-53 References

(DESIGN NOTE: Determine the appropriate columns for reporter to select from, but the first three are probably the minimum needed)

CPG #	Additional Reference(s) [including NIST 800-53 for FISMA reports]	Security Practice	Outcome	TTP or Risk Addressed	Recommended Action
2.A	NIST SP 800-53: IA-5 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	Changing default passwords	Prevent threat actors from using default passwords to achieve initial access or move laterally in a network.	Valid accounts - default accounts (T1078.001) Valid accounts (ICS T0859)	An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting on any internal or external network. This includes IT assets for operational technology, such as operational technology administration web pages. In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices. Operational technology: While changing default passwords on an

[75] Option to change default data marking

[76] Indicating that the marked data constitutes cyber threat indicator(s) or defensive measure(s) submitted under the Cybersecurity Information Sharing Act of 2015 that the submitter is requesting be treated as commercial, financial, and proprietary

[77] CUI Markings | National Archives

[78] Cross-Sector Cybersecurity Performance Goals | CISA (https://www.cisa.gov/cross-sector-cybersecurity-performance-goals)

					organization's existing operational technology requires significantly more work, we still recommend having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversary TTPs change.
2.B	NIST SP 800-53: IA-5 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 XKCD 936	Minimum password strength	Organizational passwords are harder for threat actors to guess or crack.	Brute force - password guessing (T1110.001) Brute force - password cracking (T1110.002) Brute force - password spraying (T1110.003) Brute force - credential stuffing (T1110.004)	Organizations have a system-enforced policy that requires a minimum password length of 15* or more characters for all password-protected IT assets and all operational technology assets, when technically feasible.** Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement. This goal is particularly important for organizations that lack widespread implementation of multifactor authentication (MFA) and capabilities to protect against brute-force attacks (such as web application firewalls and third-party content delivery networks) or are unable to adopt passwordless authentication methods. * Modern attacker tools can crack eight-character passwords quickly. Length is a more impactful and important factor in

					password strength than complexity or frequent password rotations. Long passwords are also easier for users to create and remember. ** Operational technology assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk operational technology assets that may not be technically feasible include those in remote locations, such as those on offshore rigs or on wind turbines.
2.C	NIST SP 800-53: AC-2, AC-3 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	Unique credentials	Attackers are unable to reuse compromised credentials to move laterally across the organization, particularly between IT and operational technology networks.	Valid accounts (T1078, ICS T0859) Brute force - password guessing (T1110.001)	Organizations provision unique and separate credentials for similar services and asset access on IT and operational technology networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/machine accounts have passwords that are unique from all member user accounts.
2.D	NIST SP 800-53: AC-2, AC-3 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	Revoking credentials for departing employees	Prevent unauthorized access to organizational accounts or resources by former employees.	Valid accounts (T1078, ICS T0859)	A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.

2.E	NIST SP 800-53: AC-6 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1	Separating user and privileged accounts	Make it harder for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised.	Valid accounts (T1078, ICS T0859)	No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are revaluated on a recurring basis to validate continued need for a given set of permissions.
2.F	NIST SP 800-53: AC-4, SC-7, SI-4 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 6.2, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3	Network segmentation	Reduce the likelihood of adversaries accessing the operations technology network after compromising the IT network.	Network service discovery (T1046) Trusted relationship (T1199) Network connection enumeration (ICS T0840) Network sniffing (T1040, ICS T0842)	All connections to the operational technology network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and operational technology networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.
2.G	NIST SP 800-53: AC-7 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10	Detection of unsuccessful (automated) login attempts	Protect organizations from automated, credential-based attacks.	Brute force - password guessing (T1110.001) Brute force - password cracking (T1110.002) Brute force - password spraying (T1110.003) Brute force - credential stuffing (T1110.004)	All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis. For IT assets, a system-enforced policy prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This

					configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10 minutes after 10 incorrect logins over a 10-minute period.
2.H	NIST SP 800-53: IA-2, IA-3 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10	Phishing-resistant MFA	Add a critical, additional layer of security to protect assets accounts whose credentials have been compromised.	Brute force (T1110) remote services - Remote desktop protocol (T1021.001) Remote services - SSH (T1021.004) Valid accounts (T1078, ICS T0859) External remote services (ICS T0822)	Organizations implement MFA for access to assets using the strongest available method for that asset (see below for scope). MFA options sorted by strength, high to low, are as follows: 1. Hardware-based, phishing-resistant MFA (e.g., FIDO/WebAuthn or public key infrastructure (PKI)-based – see CISA guidance in "Resources"); 2. If such hardware-based MFA is not available, then mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys are used; 3. MFA via short message service (SMS) or voice only used when no other options are possible. IT: All IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems. Operational technology: Within operational technology environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible Human Machine Interface (HMIs.)

2.I	NIST SP 800-53: AT-2 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1	Basic cybersecurity training	Organizational users learn and perform more secure behaviors	User training (M1017, ICS M0917)	At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security, password security, etc., as well as foster an internal culture of security and cyber awareness. New employees receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.
2.J	NIST SP 800-53: AT-3 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2	Operational technology cybersecurity training	Personnel responsible for securing operational technology assets received specialized operational technology-focused cybersecurity training	User training (M1017, ICS M0917)	In addition to basic cybersecurity training, personnel who maintain or secure operational technology as part of their regular duties receive operational technology-specific cybersecurity training on at least an annual basis.
2.K	NIST SP 800-53: SC-8, SC-13, SC-28 ISA 62443-3-3:2013 SR 3.1, SR 3.4, SR 3.8, SR 4.1, SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	Strong and agile encryption	Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and operational technology traffic	Adversary-in-the-middle (T1557) Automated collection (T1119) Network sniffing (T1040, ICS T0842) Wireless compromise (ICS T0860) Wireless sniffing (ICS T0887)	Properly configured and up-to-date secure socket layer (SSL) / transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithms, and consider managing the implications of post-quantum cryptography. Operational technology: To minimize the impact to latency and availability, encryption is used when feasible, usually for operational technology communications connecting with remote/external assets.

2.L	NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, MP-12, PE-19, PS-3, PS-6, SC-7, SC-8, SC-11, SC-12, SC-13, SC-28, SC-31, SI-4 ISA 62443-3-3:2013 SR 3.4, SR 4.1, SR 5.2 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3	Secure sensitive data	Protect sensitive information from unauthorized access	Unsecured credentials (T1552) Steal or forge Kerberos tickets (T1558) OS credential dumping (T1003) Data from information repositories (ICS T0811) Theft of operational information (T0882)	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.
2.M	NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, CM-8, MP-6, MP-8, PE-16, PE-19, PS-3, PS-6, SC-7, SC-8, SC-11, SC-12, SC-13, SC-28, SC-31, SI-4 ISA 62443-3-3:2013 SR	Email security	Reduce risk from common email-based threats, such as spoofing, phishing, and interception	Phishing (T1566) business email compromise	On all corporate email infrastructure (1) STARTTLS is enabled, (2) Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are enabled, and (3) Domain-based Message Authentication, Reporting, and Conformance (DMARC) is enabled and set to "reject." For further examples and information, see CISA's past guidance for federal agencies at <link to BOD>:

	3.1, SR 3.4, SR. 3.8, SR 4.1, SR 4.1, SR 4.2, SR 5.2				https://www.cisa.gov/binding-operational-directive-18-01
2.N	NIST SP 800-53: CM-10, CM-11, SC-13 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	Disable macros by default	Reduce the risk from embedded macros and similar executive code, a common and highly effective threat actor TTP	Phishing - spearphishing attachment (T1566.001) User execution - malicious File (T1204.002)	A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.
2.O	NIST SP 800-53: CM-2, CM-6, CM-8 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	Document device configurations	More efficiently and effectively manage, respond to, and recover from cyberattacks against the organization and maintain service continuity	Delayed, insufficient, or incomplete ability to maintain or restore functionality of critical devices and service operations.	Organizations maintain accurate documentation describing the baseline and current configuration details of all critical IT and operational technology assets to facilitate more effective vulnerability management and response and recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.
2.P	NIST SP 800-53: CM-2, CM-6, CM-8 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-	Document Network Topology	More efficiently and effectively respond to cyberattacks and maintain service continuity	Incomplete or inaccurate understanding of network topology inhibits effective incident response and recovery	Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and operational technology networks. Periodic reviews and updates should be performed and tracked on a recurring basis.

	3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4				
2.Q	NIST SP 800-53: CM-2, CM-3, CM-5, CM-6, CM-10, CM-11 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4	Hardware and software approval process	Increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software	Supply chain compromise (T1195, ICS T0862) Hardware additions (T1200) Browser extensions (T1176) Transient cyber asset (ICS T0864)	Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For operational technology assets specifically, these actions should also be aligned with defined change control and testing activities.
2.R	NIST SP 800-53: CP-6, CP-9, CP-10 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3	System Backups	Organizations reduce the likelihood and duration of data loss at loss of service delivery or operations	Data destruction (T1485, ICS T0809) Data encrypted for impact (T1486) Disk wipe (T1561) Inhibit system recovery (T1490) Denial of control (ICS T0813) Denial/loss of view (ICS T0815, T0829) Loss of availability (T0826) Loss/manipulation of control (T0828, T0831)	All systems that are necessary for operations are regularly backed up on a regular cadence (no less than once per year). Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year. Stored information for operational technology assets includes at a minimum: configurations, roles, programmable controller (PLC) logic, engineering drawings, and tools.
2.S	NIST SP 800-53: IR-3, IR-4, IR-8 ISA 62443-2-1:2009 4.3.2.5.3, 4.3.2.5.7, 4.3.4.5.1, 4.3.4.5.11	Incident Response (IR) Plans	Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios	Inability to quickly and effectively contain, mitigate, and communicate about cybersecurity incidents	Organizations have, maintain, update, and regularly drill IT and operational technology cybersecurity incident response plans for both common and organizationally-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, tests or drills are as realistic as

	ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3				feasible. IR plans are drilled at least annually and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.
2.T	NIST SP 800-53: AU-2, AU-3, AU-7, AU-9, AU-11 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks	Delayed, insufficient, or incomplete ability to detect and respond to potential cyber incidents Impair defenses (T1562)	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows event logging. Operational technology: For operational technology assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.
2.U	NIST SP 800-53: AU-2, AU-3, AU-7, AU-9, AU-11 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2,	Secure Log Storage	Organizations' security logs are protected from unauthorized access and tampering	Indicator removal on host - clear Windows event logs (T1070.001) Indicator removal on host - Clear Linux or Mac system logs (T1070.002) Indicator removal on host - file deletion (T1070.004) Indicator removal on host (ICS T0872)	Logs are stored in a central system, such as a security information and event management tool or central database and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.

	A.12.4.3, A.12.4.4, A.12.7.1				
2.V	NIST SP 800-53: MP-2, MP-7 ISA 62443-3-3:2013 SR 2.3 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9	Prohibit Connection of Unauthorized Devices	Prevent malicious actors from achieving initial access or data exfiltration via unauthorized portable media devices	Hardware additions (T1200) Replication through removable media (T1091, ICS T0847)	Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and operational technology assets, such as by limiting use of USB devices and removable media or disabling AutoRun. Operational technology: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices or establish procedures for granting access through approved exceptions.
2.W	NIST SP 800-53: AC-4, SC-7, SC-32, SC-39 ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3	No Exploitable Services on the Internet	Unauthorized users cannot gain an initial system foothold by exploiting known weaknesses in public-facing assets	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819) Exploitation of remote service (T1210, ICS T0866) External remote services (T1133, ICS T0822) Remote services - remote desktop protocol (T1021.001)	Assets on the public internet expose no exploitable services, such as remote desktop protocol. Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets.
2.X	NIST SP 800-53: AC-4, SC-7, SC-32, SC-39 ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR	Limit operational technology connections to public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet	Active scanning - vulnerability scanning (T1595.002) Exploit public-facing application (T1190, ICS T0819) Exploitation of remote service (T1210, ICS T0866)	No operational technology assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access

	5.2, SR 5.3, SR 7.1, SR 7.6 ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3			External remote services (T1133, ICS T0822)	via proxy or other intermediary, etc.).

Appendix 3: Incident Type/Categories

Incident Types involving MALWARE (based on VERIS with some modifications[79]):
Adware
Backdoor (enable remote access)
Brute force attack
Capture data from application or system process
Capture data stored on system disk
Client-side attack (client-side or browser attack (e.g., redirection, XSS, MitB))
Click fraud or Bitcoin mining
C2 (command and control)
Destroy data (destroy or corrupt stored data)
Disable controls (disable or interfere with security controls)
DoS (denial of service attack)
Downloader (pull updates or other malware)
Exploit vulnerability in code (vs misconfiguration or weakness)
Export data to another site or system
Packet sniffer (capture data from network)
Password dumper (extract credential hashes)
RAM scraper or memory parser (capture data from volatile memory)
Ransomware (encrypt or seize stored data)
Rootkit (maintain local privileges and stealth)
Scan network (scan or footprint network)
Spam (send spam)
Spyware/Keylogger (spyware, keylogger or form-grabber (capture user input or activity))
SQL injection attack
Adminware (system or network utilities (e.g., PsTools, Netcat))
Worm (propagate to other systems or devices)

Incident Types Involving Hacking (based on VERIS with some modifications [80]):
Abuse of functionality
Brute force or password guessing attacks
Buffer overflow
Cache poisoning
Session prediction: Credential or session prediction
CSRF: Cross-site request forgery
XSS: Cross-site scripting
Cryptanalysis
DoS: Denial of service
Foot-printing and fingerprinting
Forced browsing or predictable resource location

[79] Enumerations (verisframework.org)
[80] Enumerations (verisframework.org)

Format string attack
Fuzz testing
HTTP request smuggling
HTTP request splitting
Integer overflows
LDAP injection
Mail command injection
MitM: Man-in-the-middle attack
Null byte injection
Offline cracking: Offline password or key cracking (e.g., rainbow tables, Hashcat, JtR)
OS commanding
Path traversal
RFI: Remote file inclusion
Reverse engineering
Routing detour
Session fixation
Session replay
Soap array abuse
Special element injection
SQL injection
SSI injection
URL redirector abuse
Use of backdoor or C2
Use of stolen creds
XML attribute blowup
XML entity expansion
XML external entities
XML injection
XPath injection
XQuery injection
Virtual machine escape

Incident Types Involving Social Engineering (based on VERIS with some modifications [81]):
Baiting (planting infected media)
Bribery or solicitation
Elicitation (subtle extraction of info through conversation)
Extortion or blackmail
Forgery or counterfeiting (fake hardware, software, documents, etc.)
Influence tactics (leveraging authority or obligation, framing, etc.)
Scam (online scam or hoax (e.g., scareware, 419 scam, auction fraud))
Phishing (or any type of *ishing)
Pretexting (dialogue leveraging invented scenario)
Propaganda or disinformation
Spam (unsolicited or undesired email and advertisements)

Incident Types Involving Misuse of Assets [sometimes called "Insider Threats"] (based on VERIS with some modifications [82]):
Knowledge abuse: Abuse of private or entrusted knowledge

[81] Enumerations (verisframework.org)
[82] Enumerations (verisframework.org)

Privilege abuse: Abuse of system access privileges
Embezzlement, skimming, and related fraud
Data mishandling: Handling of data in an unapproved manner
Email misuse: Inappropriate use of email or IM
Net misuse: Inappropriate use of network or Web access
Illicit content: Storage or distribution of illicit content
Unapproved workaround or shortcut
Unapproved hardware: Use of unapproved hardware or devices
Unapproved software: Use of unapproved software or services

Incident Types Involving Physical Actions (based on VERIS with some modifications [83]):
Assault (threats or acts of physical violence)
Sabotage (deliberate damaging or disabling)
Snooping (sneak about to gain info or access)
Surveillance (monitoring and observation)
Tampering (alter physical form or function)
Theft (taking assets without permission)
Wiretapping (Physical tap to comms line)

Incident Types Involving Human (or Technology) Errors (based on VERIS with some modifications [84]):
Classification error (classification or labeling error)
Data entry error
Disposal error
Gaffe (social or verbal slip)
Loss or misplacement
Maintenance error
Misconfiguration
Misdelivery (direct or deliver to wrong recipient)
Omission (something intended, but not done)
Physical accidents (e.g., drops, bumps, spills)
Capacity shortage (poor capacity planning)
Programming error (flaws or bugs in custom code)
Publishing error (private info to public doc or site)
Malfunction (technical malfunction or glitch)

Incident Types Involving Environmental Factors (based on VERIS with some modifications [85]):
Deterioration and degradation
Earthquake
EMI: Electromagnetic interference (EMI)
ESD: Electrostatic discharge (ESD)
Temperature: Extreme temperature
Fire
Flood
Hazmat: Hazardous material
Humidity
Hurricane
Ice and snow
Landslide
Lightning

[83] Enumerations (verisframework.org)
[84] Enumerations (verisframework.org)
[85] Enumerations (verisframework.org)

Meteorite
Particulates: Particulate matter (e.g., dust, smoke)
Pathogen
Power failure or fluctuation
Tornado
Tsunami
Vermin
Volcanic eruption
Leak: Water leak
Wind

Appendix 4: Critical Infrastructure Sectors and Subsectors
(DESIGN NOTE: Ensure we have most approved critical infrastructure sector and subsector list per CISA data standards where applicable (Office of the Chief Information Officer - Active Data Standards - All Items (sharepoint.com))
Format of list is as follows:

- Sector
  - Subsector

- Chemical
  - Chemical manufacturing or processing plant
  - Chemical transport
  - Chemical storage warehousing and storage
  - Chemical end user
  - Regulatory, oversight, or industry organization
- Commercial facilities
  - Entertainment and media
  - Gaming
  - Lodging
  - Outdoor events
  - Public assembly
  - Real estate
  - Retail
  - Sports leagues
- Communications
  - Information services
  - Telecommunications
  - Regulatory, oversight, or industry organization
- Critical Manufacturing
  - Primary metal manufacturing
  - Machinery manufacturing
  - Electrical equipment, appliance, and component manufacturing
  - Transportation manufacturing
  - Non-critical manufacturing facility
- Dams
  - Dam project
  - Dams control operations facility
  - Levees and hurricane barriers
  - Navigation locks
  - Mine tailing and industrial waste impoundment
  - Regulatory, oversight, or industry organization
- Defense industrial base
  - Defense manufacturing facility
  - Defense research and development facility

  - Defense logistics and asset management facility
  - Defense industrial base administration and regulatory facility
- Emergency services
  - Law enforcement
  - Fire and emergency services
  - Emergency medical services
  - Emergency management
  - Public works
  - Emergency communication
- Energy
  - Electricity
  - Petroleum
  - Natural gas
  - Coal
  - Ethanol
  - Biodiesel
  - Hydrogen
- Financial Services
  - Banking and credit
  - Securities, commodities, or financial investment
  - Insurance company
- Food and agriculture
  - Supply
  - Processing, packaging, and production
  - Agriculture and food product storage and distribution warehouse
  - Agriculture and food product transportation
  - Agriculture and food product distribution
  - Agriculture and food supporting facility
  - Regulatory, oversight, or industry organization
- Government facilities
  - Elections facilities
  - K-12 education facilities
  - Government education facility
  - Military facility
  - National monument & icon
  - Personnel-oriented government facility
  - Service-oriented government facility
  - Government sensor or monitoring facility
  - Government space facility
  - Government storage or preservation facility
- Healthcare and public health
  - Direct patient healthcare
  - Health information technology
  - Fatality/mortuary services
  - Medical materials
  - Laboratories, blood, and pharmaceuticals
  - Public health services
  - Healthcare educational facility
  - Regulatory, oversight, or industry organization
- Information technology
  - Hardware production
  - Software production
  - Operational support service facility

  - Internet-based content, information, and communications services
- Nuclear reactors, materials, and waste
  - Nuclear reactor facility
  - Nuclear material processing and handling facility
  - Nuclear waste facility
- Transportation systems
  - Aviation
  - Maritime
  - Freight rail
  - Highway and motor carrier
  - Pipeline
  - Postal and shipping
  - Mass transit
- Water and wastewater systems
  - Drinking water
  - Wastewater
  - Regulatory, oversight, or industry organization

Appendix 5: Federal Agencies and Sub-Agencies

Format of list is as follows:

- Agency
    - Sub-agency

- Advisory Council on Historic Preservation (ACHP)
- African Development Foundation (ADF)
- American Battle Monuments Commission (ABMC)
- Appalachian Regional Commission (ARC)
- Armed Forces Retirement Home
- Broadcasting Board of Governors (BBG)
    - International Broadcasting Bureau
- Central Intelligence Agency (CIA)
- Chemical Safety and Hazard Investigation Board (CSHIB)
- Commission of Fine Arts (CFA)
- Commission on Civil Rights (CCR)
- Commodity Futures Trading Commission (CFTC)
- Congressional Budget Office
- Consumer Financial Protection Bureau (CFPB)
- Consumer Product Safety Commission (CPSC)
- Corporation for National and Community Service (CNCS)
    - Office of Information Technology
- Court Services and Offender Supervision Agency (CSOSA)
- Defense Nuclear Facilities Safety Board (DNFSB)
- Delaware River Basin Commission (DRBC)
- Department of Agriculture (USDA)
    - Agricultural Marketing Service (AMS)
    - Agricultural Research Service
    - Animal & Plant Health Inspection Service
    - Assistant Secretary for Administration
    - Assistant Secretary for Congressional Relations
    - Chief Financial Officer
    - Chief Information Officer (CIO)
    - Cooperative State Research, Education, and Extension Service
    - Departmental Administration
    - Director of Communications
    - Economic Research Service
    - Executive Operations
    - Farm Service Agency
    - Food and Nutrition Service
    - Food Safety Inspection Service
    - Foreign Agricultural Service (FAS)
    - Forest Service
    - General Counsel
    - Grain Inspection, Packers and Stockyard Administration
    - Hawaii Agricultural Research Center
    - Information Technology Services (ITS)
    - Inspector General
    - National Agricultural Library
    - National Agriculture Statistics Service
    - National Finance Center (NFC)
    - Natural Resources Conservation Service

  - Office of Communication
  - Office of the Secretary
  - Research, Economics & Education
  - Risk Management
  - Rural Development
  - Telecommunications Services and Operations (TSO)
  - Under Secretary for Farm and Foreign Agricultural Services
  - Under Secretary for Food Nutrition and Consumer Services
  - Under Secretary for Food Safety
  - Under Secretary for Marketing and Regulatory Programs
  - Under Secretary for Natural Resources and Environment
  - Under Secretary for Research Education and Economics
  - Under Secretary for Rural Development
- Department of Commerce (DOC)
  - Bureau of Economic Analysis (BEA)
  - Bureau of Export Administration
  - Bureau of Industry and Security
  - Bureau of the Census
  - Chief Information Officer (CIO)
  - DOC-CIRT
  - Economic Development Administration
  - Economics and Statistics Administration
  - FEDWorld
  - International Trade Administration (ITA)
  - Minority Business Development Agency
  - National Institute of Standards & Technology (NIST)
  - National Marine Fisheries Service (NMFS)
  - National Ocean Service
  - National Oceanic & Atmospheric Administration (NOAA)
  - National Technical Information Service (NTIS)
  - National Telecommunications & Information Administration
  - National Weather Service
  - Office of Inspector General
  - Office of the Secretary
  - Patent and Trademark Office
  - Technology Administration
  - U.S. Patent and Trademark Office
- Department of Defense (DOD)
  - Air Force (USAF)
  - American Forces Press Service
  - Army (USA)
  - Chief Information Officer (CIO)
  - Defense Commissary Agency
  - Defense Contract and Audit Agency (DCAA)
  - Defense Finance and Accounting Service (DFAS)
  - Defense Information Systems Agency (DISA)
  - Defense Intelligence Agency (DIA)
  - Defense Logistics Agency (DLA)
  - Defense Security Service
  - Defense Technical Information Center (DTIC)
  - Joint Chiefs of Staff (JCS)
  - Joint Task Force-Global Network Operations (JTF-GNO)
  - Marine Corps (USMC)

- Missile Defense Agency (MDA)
- National Guard
- National Security Agency (NSA)
- Navy (USN)

- Department of Education (EDUC)
  - Chief Information Officer (CIO)
  - Educational Resources Information Center (ERIC)
  - Federal Student Aid (FSA)
  - National Library of Education (NLE)
  - Office of Educational Technology
  - Office of General Counsel
  - Office of Inspector General
  - Office of Intergovernmental and Interagency Affairs
  - Office of Legislation and Congressional Affairs
  - Office of Management
  - Office of Public Affairs
  - Office of the Chief Financial Officer
  - Office of the Chief Information Officer
  - Office of the Secretary
- Department of Energy (DOE)
  - Ames Laboratory
  - Argonne National Laboratory (ANL)
  - Assistant Secretary for Congressional and Intergovernmental
  - Assistant Secretary for Environment Safety and Health (ES&H)
  - Assistant Secretary for Environmental Management
  - Assistant Secretary for Fossil Energy
  - Assistant Secretary for Policy and International Affairs
  - Associate Administrator for Facilities and Operations
  - Associate Administrator for Management and Administration
  - Brookhaven National Lab
  - Chief Information Officer (CIO)
  - Computer Incident Advisory Capability (CIAC)
  - Defense Nuclear Facilities Safety Board Liaison
  - Deputy Administrator for Defense Nuclear Nonproliferation
  - Deputy Administrator for Defense Programs
  - Deputy Administrator for Naval Reactors
  - Energy Information Administration
  - Federal Energy Regulatory Commission
  - FermiLab
  - General Counsel
  - Idaho National Labs
  - Lawrence Berkeley National Laboratory
  - Lawrence Livermore National Laboratory
  - Los Alamos National Laboratory
  - Oak Ridge National Labs
  - Office of Civilian Radioactive Waste Management
  - Office of Counterintelligence
  - Office of Economic Impact and Diversity
  - Office of Emergency Operations
  - Office of Hearings and Appeals
  - Office of Independent Oversights and Performance Assurance
  - Office of Intelligence
  - Office of Management Budget and Evaluation/Chief Financial

  - Office of Nuclear Energy Science and Technology
  - Office of Public Affairs
  - Office of Science
  - Office of Security
  - Office of the Inspector General
  - Office of the Secretary
  - Office of Worker and Community Transition
  - Power Marketing Administrations
  - Secretary of Energy Advisory Board
  - Southwestern Power Administration
  - Under Secretary for Energy Science and Environment
  - Under Secretary for Nuclear Security
- Department of Health and Human Services (HHS)
  - Administration for Children and Families
  - Administration on Aging
  - Agency for Healthcare Research and Quality (AHCRQ)
  - Agency for Toxic Substances and Disease Registry
  - Centers for Disease Control and Prevention (CDC)
  - Centers for Medicare and Medicaid Services (CMS)
  - Chief Information Officer (CIO)
  - Financial Management Systems
  - Food and Drug Administration (FDA)
  - Health Resources and Services Administration
  - Indian Health Service
  - National Institutes of Health (NIH)
  - Office of Inspector General
  - Office of the Secretary
  - Program Support Center
  - Secure One Communications Center (SOCC)
  - Substance Abuse and Mental Health Services Administration
- Department of Homeland Security (DHS)
  - Bureau of Citizenship and Immigration Services
  - Chief Information Officer (CIO)
  - Cybersecurity and Infrastructure Security Agency (CISA)
  - CSIRC
  - Customs & Border Protection
  - Federal Emergency Management Agency (FEMA)
  - Federal Law Enforcement Training Center
  - Federal Protective Service (FPS)
  - Headquarters
  - HSOC
  - Immigration and Customs Enforcement (ICE)
  - Information Analysis Infrastructure Protection (IAIP)
  - National Coordinating Center (NCC Watch)
  - National Infrastructure Coordination Center (NICC)
  - NCSD
  - Office of Immigration Statistics
  - Office of the Inspector General (OIG)
  - Science and Technology Directorate
  - Transportation Security Administration (TSA)
  - United States Coast Guard
  - United States Secret Service
- Department of Housing and Urban Development (HUD)

  - Administration
  - Chief Financial Officer
  - Chief Information Officer (CIO)
  - Chief Procurement Officer
  - Community Planning and Development
  - Congressional and Intergovernmental Relations
  - Enforcement Center
  - Federal Housing Enterprise Oversight
  - General Counsel
  - Government National Mortgage Association (Ginnie Mae)
  - Housing and Urban Development Reading Room
  - Inspector General
  - Multifamily Housing Assistance Restructuring
  - Office of Departmental Equal Employment Opportunity
  - Office of Departmental Operations and Coordination
  - Office of Healthy Homes and Lead Hazard Control
  - Office of the Secretary
  - Policy Development and Research
  - Public Affairs
  - Public and Indian Housing
  - Real Estate Assessment Center
- Department of Justice (DOJ)
  - Antitrust Division (ATR)
  - Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
  - Civil Division
  - Civil Rights Division
  - Community Relations Service
  - Criminal Division
  - DOJCERT
  - Drug Enforcement Agency (DEA)
  - Environment and Natural Resources Division
  - Executive Office for Immigration Review
  - Executive Office for the U.S. Attorneys
  - Executive Office for the U.S. Trustees
  - Federal Bureau of Investigation (FBI)
  - Federal Bureau of Prisons
  - Inspector General
  - Intelligence Policy and Review
  - Intergovernmental Affairs
  - Justice and Management Division
  - Legal Counsel
  - Legal Policy
  - Legislative Affairs
  - National Drug Intelligence Center (NDIC)
  - Office of Community Oriented Policing Services
  - Office of Federal Detention Trustee (OFDT)
  - Office of Information & Privacy (OIP)
  - Office of Justice Programs (OJP)
  - Office of Professional Responsibility (OPR)
  - Office of the Associate Attorney General
  - Office of the Attorney General
  - Office of the Deputy Attorney General
  - Office of the Pardon Attorney

  - Office of the Solicitor General
  - Public Affairs
  - Tax Division
  - U.S. National Central Bureau - INTERPOL (USNCB)
  - U.S. Parole Commission
  - U.S. Trustee Program (USTP)
  - United States Marshals Service (USMS)
- Department of Labor (DOL)
  - Administration Review Boards (ARB)
  - Benefits Review Board (BRB)
  - Bureau of International Labor Affairs (ILAB)
  - Bureau of Labor Statistics (BLS)
  - Center for Faith-Based and Community Initiatives
  - Employee Benefit Securities Administrations (EBSA)
  - Employee's Compensation Appeals Board (ECAB)
  - Employment Standards Administration (ESA)
  - Employment Training Administration (ETA)
  - Mine Safety Health Administration (MSHA)
  - National Mine Health and Safety Academy
  - Office of Congressional and Intergovernmental Affairs
  - Office of Disability Employment Policy (ODEP)
  - Office of Job Corps (OJC)
  - Office of Public Affairs (OPA)
  - Office of Safety and Health Administration (OSHA)
  - Office of Small Business Programs (OSBP)
  - Office of the Administrative Law Justices (ALJ)
  - Office of the Assistant Secretary for Policy (OASP)
  - Office of the Chief Financial Officer (OCFO)
  - Office of the Inspector General (OIG)
  - Office of the Secretary (OSEC)
  - Office of the Solicitor of Labor (SOL)
  - Veterans Employment and Training Service (VETS)
  - Women's Bureau (WB)
- Department of State (DOS)
  - Agricultural Economics and Business Affairs
  - Appellate Review Board
  - Board of the Foreign Service
  - Bureau of Diplomatic Security
  - Chief Information Officer (CIO)
  - Commissions
  - Coordinator for Counterterrorism
  - Counselor of the Department
  - Country Officers
  - Democracy Human Rights and Labor Bureau
  - Department of State Library
  - Deputy Secretary
  - Examiners for the Foreign Service
  - Executive Secretariat
  - Foreign Service Grievance Board
  - Historian
  - Intelligence and Research
  - Legal Adviser
  - Legislative Affairs

  - NATO (North Atlantic Treaty Organization)
  - Office of the Secretary
  - Office of the United Nations Ambassador
  - Policy Planning Staff
  - Under Secretary for Arms Control and International Security
  - Under Secretary for Global Affairs
  - Under Secretary for Management
  - Under Secretary for Political Affairs
  - Under Secretary for Public Diplomacy and Public Affairs
  - United National Political Affairs
- Department of the Interior (DOI)
  - Bureau of Indian Affairs
  - Bureau of Land Management
  - Bureau of Reclamation
  - Chief Information Officer (CIO)
  - DOI CIRC
  - Fish and Wildlife Service
  - Minerals Management Service
  - National Business Center
  - National Park Service
  - Office of Hearings and Appeals
  - Office of Surface Mining
  - Office of the Inspector General
  - Office of the Secretary
  - US Geological Survey
- Department of the Treasury
  - Alcohol and Tobacco Tax and Trade Bureau (TTB)
  - Bureau of Alcohol Tobacco and Firearms (ATF)
  - Bureau of Engraving and Printing
  - Bureau of the Fiscal Service (BFS)
  - Chief Information Officer (CIO)
  - Comptroller of the Currency
  - Executive Office for Asset Forfeiture
  - Federal Law Enforcement Training Center
  - Financial Crimes Enforcement Network
  - Internal Revenue Service (IRS)
  - Office of the Comptroller of the Currency
  - Office of the Inspector General
  - Office of the Secretary
  - Office of Thrift Supervision (OTS)
  - TCSIRC
  - Treasury Headquarters (Treas-HQ)
  - United States Customs Services
  - United States Mint
  - US Federal Civilian Agency
- Department of Transportation (DOT)
  - Bureau of Transportation Statistics
  - Chief Information Officer (CIO)
  - Federal Aviation Administration (FAA)
  - Federal Highway Administration
  - Federal Motor Carrier Safety Administration
  - Federal Railroad Administration
  - Federal Transit Administration

  - Maritime Administration
  - National Highway Traffic Safety Administration
  - Office of the Inspector General
  - Office of the Secretary
  - Research and Special Programs Administration
  - Saint Lawrence Seaway Development Corporation
  - Surface Transportation Board
  - Transportation Administrative Services Center
  - Transportation CIRC (TCIRC)
- Department of Veterans Affairs
  - Acquisition and Material Management
  - Acute Care Strategic Healthcare Group
  - Administration and Human Resources
  - Allied Clinical Services Strategic Healthcare Group
  - Audit
  - Austin Automation Center
  - Board of Contract Appeals
  - Board of Veterans' Appeals
  - Budget
  - Chief Information Officer (CIO)
  - Congressional and Legislative Affairs
  - Deputy Secretary
  - Disadvantaged and Small Business Utilization
  - Diversity Management and Equal Employment Opportunity
  - Emergency Management Strategic Healthcare Group
  - Employee Education
  - Facilities Management
  - Facilities Service
  - General Counsel
  - Geriatrics and Extended Care Strategic Healthcare Group
  - Information and Technology
  - Inspector General
  - Intergovernmental and Public Affairs
  - Law Enforcement and Security
  - Litigation Docket
  - Management
  - National Cemetery Administration
  - Nursing Strategic Healthcare Group
  - Office of Dentistry
  - Office of Investigations
  - Office of the Secretary
  - Patient Care Services
  - Planning and Elution
  - Planning and Policy
  - Policy Office
  - Primary and Ambulatory Care Strategic Healthcare Group
  - Quality and Performance Office
  - Readjustment Counseling Service
  - Rehabilitation Strategic Healthcare Group
  - Research and Development
  - Support Service
  - Telecommunications
  - VACIRC

    - VASOC
    - Veterans Benefits Administration
    - Veterans Health Administration
- Environmental Protection Agency (EPA)
- Equal Employment Opportunity Commission (EEOC)
- Executive Office of the President (EOP)
    - Office of Management and Budget (OMB)
    - United States Trade Representative (USTR)
    - White House
- Export-Import Bank of the United States (EIIM)
- Fannie Mae (FNMA)
- Farm Credit Administration (FCA)
- Federal Accounting Standards Advisory Board (FASAB)
- Federal Communications Commission (FCC)
- Federal Deposit Insurance Corporation (FDIC)
- Federal Election Commission (FEC)
- Federal Energy Regulatory Commission (FERC)
- Federal Housing Finance Agency (FHFA)
- Federal Judiciary
    - Administrative Office of the United States Courts
- Federal Labor Relations Authority (FLRA)
- Federal Maritime Commission (FMC)
- Federal Mediation and Conciliation Service (FMCS)
- Federal Mine Safety and Health Review Commission (FMSHRC)
- Federal Reserve System (FRS)
    - Board of Governors
- Federal Retirement Thrift Investment Board (FRTIB)
    - Thrift Savings Plan
- Federal Trade Commission (FTC)
- Freddie Mac (FHLMC)
- General Services Administration (GSA)
- Government Printing Office
- Harry S Truman Scholarship Foundation (HTSF)
- Holocaust Memorial Council (HMC)
- House of Representatives
- Independent Agencies
    - United States Consumer Product Safety Commission (CPSC)
- Institute of Museum and Library Services (IMLS)
- Institute of Peace United States (USIP)
- Inter-American Foundation (IAF)
- International Boundary and Water Commission
- International Broadcasting Bureau (IBB)
- International Trade Commission (ITC)
- ISAC
    - Airport
    - Chemical
    - Electricity
    - Emergency Fire Services
    - Energy
    - Financial Services (FS)
    - Food and Agriculture

    - Information Technology (IT)
    - Maritime
    - Multi-State (MS)
    - National Monuments and Icons
    - Postal and Shipping
    - Public Health
    - Real Estate
    - Research and Education
    - State CIO
    - Surface Transportation
    - Telecom
    - Trucking
    - Water
- James Madison Memorial Fellowship Foundation (JMMFF)
- Japan - United States Friendship Commission (JUSFC)
- Javits-Wagner-O'Day Program (JWOD)
- Legal Services Command (LSC)
- Library of Congress
- Marine Mammal Commission (MMC)
- Merit Systems Protection Board (MSPB)
- Millennium Challenge Corporation (MCC)
- National Aeronautics and Space Administration (NASA)
    - Ames Research Center (ARC)
    - Chief Information Officer (CIO)
    - Glenn Research Center (GRC)
    - Goddard Space Flight Center (GSFC)
    - Jet Propulsion Laboratories (JPL)
    - Johnson Space Center (JSC)
    - Kennedy Space Flight Center (KSFC)
    - Langley Research Center (LRC)
    - Marshall Space Flight Center (MSFC)
    - NASIRC
    - Stennis Space Center
    - Wallops Flight Facility (WFF)
- National Archives and Records Administration (NARA)
- National Capital Planning Commission (NCPC)
- National Council on Disability (NCD)
- National Credit Union Administration (NCUA)
- National Endowment for the Arts
- National Endowment for the Humanities
- National Foundation on the Arts and the Humanities (NFAH)
- National Gallery of Arts (NGA)
- National Indian Gaming Commission (NIGC)
- National Institute for Literacy
- National Labor Relations Board (NLRB)
- National Mediation Board (NMB)
- National Railroad Passenger Corporation (AMTRAK)
- National Science Foundation (NSF)
    - US Climate Change Science Program (USGCRP)
- National Transportation Safety Board (NTSB)
- Neighborhood Reinvestment Corporation (NBRC)

- Nuclear Regulatory Commission (NRC)
- Nuclear Waste Technical Review Board United States (NWTRB)
- Occupational Safety and Health Administration (OSHA)
- Occupational Safety and Health Review Commission (OSHRC)
- Office of Federal Housing Enterprise Oversight (OFHEO)
- Office of Government Ethics (OGE)
- Office of Navajo & Hopi Indian Relocation
- Office of Personnel Management
- Office of Special Counsel (OSC)
- Office of the Director of National Intelligence (ODNI)
    - Information Sharing Environment (ISE)
    - Intelligence Advanced Research Projects Activity (IARPA)
    - National Counterproliferation Center (NCPC)
    - National Counterterrorism Center (NCTC)
    - National Intelligence Council (NIC)
    - Office of the National Counterintelligence Executive (ONCIX)
- Open Source Information System (OSIS)
- Peace Corps (PC)
- Pension Benefit Guaranty Corporation (PBGC)
- Postal Rate Commission (PRC)
- Railroad Retirement Board (RRB)
- Recovery Accountability and Transparency Board
- Securities and Exchange Commission (SEC)
- Selective Service System (SSS)
- Small Business Administration (SBA)
- Smithsonian Institute (SI)
- Social Security Administration (SSA)
- State Justice Institute (SJI)
- Susquehanna River Basin Commission (SRBC)
- Tennessee Valley Authority (TVA)
- U.S. International Development Finance Corporation (DFC)
- U.S. Senate
- U.S. Trade and Development Agency (TDA)
- United States Agency for International Development (USAID)
- United States Arms Control and Disarmament Agency (ACDA)
- United States Congress
    - Government Accountability Office (GAO)
- United States International Trade Commission (USITC)
- United States Postal Service (USPS)
- United States Trade and Development Agency
- US-China Economic and Security Review Commission (USCC)
- Voice of America (VOA)