CISA Incident Reporting Form
Complete Question Set

Table of Contents

a. Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) collects cybersecurity incident reports related to federal agency information systems, mandatory reports on behalf of certain federal regulatory agencies, mandatory reports due to contractual requirements, and voluntary reports from members of the public. This question set, which is authorized by the Federal Information Security Modernization Act of 2014 (FISMA) and the Homeland Security Act, is distinct from incident reporting under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). CISA will use a different information collection instrument for CIRCIA incident reports after the effective date of CIRCIA implementing regulations.

The questions included in this document represent the universe of all possible questions CISA may use for incident report information collection purposes across the multiple existing incident reporting use cases; no respondent will be presented all the questions. In the Incident Reporting Portal respondents will be directed to answer a subset of the questions based on the characteristics of the reporting entity, the reasons for which they are reporting, and the nature of the incident. The dynamic design of the Incident Reporting Portal means that the user experience flow from question to question is driven by the individual respondent's responses. As described in the next section CISA has provided design notes to explain the conditional logic which supports the dynamic design; the conditional logic may change as CISA works to implement the Incident Reporting Portal and is provided as an example to help the reader understand how questions relate to one another.

b. Labels Used

Throughout this document labels are used to provide context on how conditional logic may impact the flow from question-to-question, to indicate where certain respondents may be able to indicate they would like certain data markings applied to their responses to the question, and to note where additional text may be shown to the respondent in the Incident Reporting Portal to assist with question comprehension.

Conditional Logic Markings:

[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.

[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.

{Conditional} = Provides additional conditional logic context on some questions.

Data Markings:

[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 note markings:

Display notes do not contain questions with which a respondent must engage. Display notes contain additional explanatory content which may assist a respondent with responding to a question. The format for these notes is as follows:

> **(DISPLAY NOTE: Light blue and bolded words should be displayed to the reader.)**
>
> All Footnotes contained in this document accompany Display Notes and 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.

Design notes are intended to enable the developers of the Incident Reporting Portal and reviewers of the question understand the conditional logic which may direct a respondent from one question to the appropriate next question based on their input. The flow from question-to-question will continue to be under development as CISA incorporates feedback from reviewers. However, since it is critical to communicate that no respondent will answer all the questions contained herein, we wanted to provide this conditional logic to support reviewers' understanding of how the dynamic form may work. The format for these notes is as follows:

> **(DESIGN NOTE: Black and bolded words are for the developers only and should not be displayed to the readers.)**

c. 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.)

d. Report Type

FOR ALL REPORTERS

1. [RA] What type of report do you want to submit?
   A. Initial report
   B. Supplemental/update report
   C. Post-incident report[1]

e. Report Reason

2. [RA] Why are you reporting? **(DESIGN NOTE: Single select)**
   A. Voluntarily reporting a cyber incident (select one) **(DESIGN NOTE: If voluntary is selected, display the two following types of voluntary reporting and single select)**
      1. Are you voluntarily reporting an incident for an individual (yourself or another person)?
      2. Are you voluntarily reporting an incident for an entity (a company, organization[2], etc.)?
   B. 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.)
3. {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)**

   (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.)
   A. Cybersecurity and Infrastructure Security Agency (CISA)
      1. Federal Information Security Modernization Act of 2014 (FISMA 2014)
         a. Please select the appropriate report reason:
            1. Cyber incident
            2. Unauthorized release and/or loss of agency information (including personally identifiable information) unrelated to a cybersecurity incident

   B. Federal Energy Regulatory Commission (FERC)/ North American Electric Reliability Corporation (NERC)

[1] **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.

[2] 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.

1. Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security Management Controls) and CIP-008-6 (Cyber Security – Incident Reporting and Response Planning)

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

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

E. Transportation Security Administration (TSA)
   1. 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)
   2. Security Directives or Information Circulars associated with Pipeline Cybersecurity (SD Pipeline 2021-01 series and IC Pipeline 2022-01, including all amendments and successors)
   3. (**DESIGN NOTE: Placeholder for aviation citations, details TBD**)
      a. Airport Security Program (ASP)
      b. Aircraft Operator Standard Security Program (AOSSP)
      c. Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP)
      d. Twelve-Five Standard Security Program (TFSSP)
      e. Private Charter Standard Security Program (PCSSP)
      f. Indirect Air Carrier Standard Security Program (IACSSP)
      g. Certified Cargo Screening Standard Security Program (CCSSP)

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

G. Reserved entity for future if necessary {PRA placeholder}
   1. Reserved statute, regulation, or contractual requirement
      a. Please select the appropriate report reason:
         1. (**DESIGN NOTE: "report reason" List**)

H. 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.**)
   1. Agency [describe] **(DESIGN NOTE: Open text)**
   2. Statute, regulation, or contract clause [describe] **(DESIGN NOTE: Open text)**

f. Contact Information of Reporter:

4. [CUI][RA] Please provide your name and contact information
   A. [CUI]Name
      1. First
      2. Last
   B. [CUI] Phone number(s)
      1. Preferred
      2. Alternate
   C. [CUI] Email address(es)
      1. Preferred
      2. Alternate
   D. [CUI] Social media profile (Optional)
      1. Primary social media handle or username?
      2. Enter the corresponding social media platform
   E. Job title
   F. Which time zone are you in?

5. [CUI][RA] Are you the primary point of contact for this incident? (Yes/No)
   A. [CUI][RC] **(DESIGN NOTE: If No)** Please provide the primary point of contact name and contact information
      1. [CUI]Name
         a. First
         b. Last
      2. [CUI]Phone number(s)
         a. Preferred
         b. Alternate
      3. [CUI]Email address(es) of point of contact
         a. Preferred
         b. Alternate
      4. [CUI] Social media profile (Optional)
         a. Primary social media handle or username?
         b. Enter the corresponding social media platform
      5. Job title
      6. Which time zone are they in?

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

7. [RA] Do you work for the affected entity?
   A. Not applicable, I am an individual, self-reporting an incident affecting me.
   B. Yes
   C. Yes, 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.)**
      1. [CUI]Please provide the contact information for the person at the impacted entity who expressly authorized you to report on the entity's behalf.
         a. [CUI]Name
            1. First
            2. Last
         b. [CUI]Phone number(s)
            1. Preferred
            2. Alternate
         c. [CUI] Email address(es) of point of contact
            1. Preferred
            2. Alternate
         d. Job title
   D. No, I am a third party and do **not** have the consent and/or have **not** been expressly authorized to report on the affected entity's behalf (law firm, incident response firm, etc.) **(DISPLAY NOTE: If a third party is submitting a report on behalf of the impacted entity without consent and/or authorization, this incident will be validated between the impacted entity and CISA.)**

g. Impacted Entity Demographics

8. [RA] What is the affected entity type?
   A. Private sector (including U.S. Government contractors)
   B. U.S. Federal Government agency
   C. U.S. State, Local, Tribal, or Territorial (SLTT) entity
   D. Foreign government entity
   E. Civil society
   F. Other [describe]
9. [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
   A. Please provide the name of the affected entity. (Please spell out any acronyms.)
      1. Is the affected entity a subsidiary of a larger entity? (Yes/No) **(DESIGN NOTE: If Yes)** Provide the name of the larger/parent entity
   B. Is the affected entity operating in a critical infrastructure sector[3]? (Yes/No)
      1. {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[4], 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)
         a. 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:
            1. 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.

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

2. 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.
3. 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.

b. (**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. (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.))**

1. If you do not wish to have your submission evaluated as a PCII submission, please check this box [ ]

c. (**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.)**

2. **(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-subsector. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list.)**
    a. Chemical
    b. Commercial Facilities
    c. Communications
    d. Critical Manufacturing
    e. Dams
    f. Defense Industrial Base
    g. Emergency Services
    h. Energy
    i. Financial Services
    j. Food and Agriculture
    k. Government Facilities
    l. Healthcare and Public Health
    m. Information Technology
    n. Nuclear Reactors, Materials, and Waste

o. Transportation Systems
p. Water and Wastewater Systems
q. Unsure

3. **(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.)**

10. [RC] **(DESIGN NOTE: Applies to only "U.S. Federal Government agency" selection)** U.S. Federal Government agency – Impacted Entity Demographics
    A. Please provide the Federal agency name **(DESIGN NOTE: Select from list in Appendix 5)**[5]
        1. Please select your sub-agency below after selecting your parent agency (if applicable)**(DESIGN NOTE: Select from list in Appendix 5)**[6]**)**
    B. We understand all incidents occurring at federal agencies impact the Government facilities critical infrastructure sector[7] 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)**
        1. Chemical
        2. Commercial Facilities
        3. Communications
        4. Critical Manufacturing
        5. Dams
        6. Defense Industrial Base
        7. Emergency Services
        8. Energy
        9. Financial Services
        10. Food and Agriculture
        11. Government Facilities

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

12. Healthcare and Public Health
13. Information Technology
14. Nuclear Reactors, Materials, and Waste
15. Transportation Systems
16. Water and Wastewater Systems
17. Unsure

C. 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.)**

11. [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

A. 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)**

1. [ ] State or territory
    a. Please provide the impacted entity's name (spell out any acronyms)
    b. Please select your state or territory below **(DESIGN NOTE: Select from list)**.[8]

2. [ ] Local
    a. 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:
        1. Please provide the impacted entity's name (spell out any acronyms)
        2. Please select the associated state or territory below **(DESIGN NOTE: Select from list)**.[9]
3. [ ] Tribal
    a. Tribal governments or communities, please indicate your tribe's name and any U.S. states and/or territories where the tribe is physically located.

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

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

1. Please provide the impacted entity's name
2. Please provide the associated U.S. states or territories for reference
    i. Please select the associated states or territories below **(DESIGN NOTE: Select from list)** [10] **(DESIGN NOTE: Allow more than one entry as a tribe maybe physically spread across several states and regions)**

B. Is the impacted SLTT Entity in a critical infrastructure sector?[11] (Yes/No)
    1. {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[12], 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)
        a. 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:
            1. 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.
            2. 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.
            3. Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair,

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

recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

b. (**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. (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".))**

1. If you do not wish to have your submission evaluated as a PCII submission, please check this box [ ]

c. (**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.)**

2. **(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.)**
    1. Chemical
    2. Commercial Facilities
    3. Communications
    4. Critical Manufacturing
    5. Dams
    6. Defense Industrial Base
    7. Emergency Services
    8. Energy
    9. Financial Services
    10. Food and Agriculture
    11. Government Facilities
    12. Healthcare and Public Health
    13. Information Technology
    14. Nuclear Reactors, Materials, and Waste
    15. Transportation Systems
    16. Water and Wastewater Systems
3. **(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.)**

12. [RC] **(DESIGN NOTE: Applies to only "Foreign Government Entity" selection)** **Foreign Government Entity – Impacted Entity Demographics**
    A. Please provide details about the impacted foreign entity
        1. Please select your country below (select from list)[13]
        2. Please provide the impacted entity's name (spell out any acronyms)
        3. Is your entity a computer security incident response team (CSIRT)? (Yes/No)
            a. **(DESIGN NOTE: If Yes, show question)** Please enter the name of the CSIRT **(DESIGN NOTE: Open text)**
    B. Is the impacted entity in a critical infrastructure sector[14] (based on U.S. designation) (Yes/No)
            a. **(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.)**
                1. Chemical
                2. Commercial Facilities
                3. Communications
                4. Critical Manufacturing
                5. Dams
                6. Defense Industrial Base
                7. Emergency Services
                8. Energy
                9. Financial Services
                10. Food and Agriculture
                11. Government Facilities
                12. Healthcare and Public Health
                13. Information Technology
                14. Nuclear Reactors, Materials, and Waste
                15. Transportation Systems
                16. Water and Wastewater Systems
                17. Unsure
            b. **(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?

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

(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.)**

13. [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**
    A. Please provide the impacted Federal agency you are supporting **(DESIGN NOTE: Select from list in Appendix 5)** [15]
        1. Please select the sub-agency below, if applicable) **(DESIGN NOTE: Select from list in Appendix 5)** [16]
    B. 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.
        a. **(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.)**
            1. Chemical
            2. Commercial Facilities
            3. Communications
            4. Critical Manufacturing
            5. Dams
            6. Defense Industrial Base
            7. Emergency Services
            8. Energy
            9. Financial Services
            10. Food and Agriculture
            11. Government Facilities
            12. Healthcare and Public Health
            13. Information Technology
            14. Nuclear Reactors, Materials, and Waste

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

15. Transportation Systems
16. Water and Wastewater Systems
17. Unsure

b. 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 incident. If applicable, also select the appropriate critical infrastructure-subsector. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list.)**

C. [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)**

1. Contract number(s)
2. Contract or other agreement clearance level
    a. Unclassified
    b. Confidential
    c. Secret
    d. Top Secret
    e. Not Applicable
3. [Fed Ctr] Has the impacted entity been granted a facility security clearance? (Yes/No)
    a. **(DESIGN NOTE: If Yes)** [Fed Ctr] What is the facility clearance level (FCL) of the impacted entity?
        1. Unclassified
        2. Confidential
        3. Secret
        4. Top Secret (may or may not include Sensitive Compartmented Information)
        5. Not applicable
4. [Fed Ctr] Are you the prime contractor under this contract? (Yes/No)
    a. **(DESIGN NOTE: If No)** Please provide the prime contractor point of contact
        1. Name
            i. First
            ii. Last

2. Phone number(s)
3. Email address(es)
4. Position/title
5. Address
    i. Street name and number
    ii. Postal code
    iii. City
    iv. State
    v. Country
    vi. Time zone

5. [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)[17] and US Government Program Manager (PM).) (DESIGN NOTE: Allow for more than one entry)**
    a. Name
        1. First
        2. Last
    b. Phone number(s)
    c. Email address(es)
    d. Position/title[18] (e.g., CO, COR, ACO, PM) **(DESIGN NOTE: Provide "dropdown list" to select from example list, allow "OTHER" with a fill-in description)**
    e. Address
        1. Street name and number
        2. Postal code
        3. City
        4. State
        5. Country
        6. Time zone

14. [RC] **(DESIGN Note: Applies to only "civil society" selection) Civil Society – Impacted Entity Demographics**

A. Please provide details about the impacted civil society entity

[17] 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

[18] 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 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.)

1. 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)**
2. Please enter the civil society entity's name (spell out any acronyms)

B. Are there any critical infrastructure (critical infrastructure) sector(s)[19] directly impacted by the incident that occurred/is occurring at your organization? (Yes/No)
   1. {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[20], 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)
      a. 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:
         1. 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.
         2. 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.
         3. Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the

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

extent it is related to such interference, compromise, or incapacitation.

b. (**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.** **(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".))**

1. If you do not wish to have your submission evaluated as a PCII submission, please check this box [ ]

c. (**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.)**

2. **(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.)**
    a. Chemical
    b. Commercial Facilities
    c. Communications
    d. Critical Manufacturing
    e. Dams
    f. Defense Industrial Base
    g. Emergency Services
    h. Energy
    i. Financial Services
    j. Food and Agriculture
    k. Government Facilities
    l. Healthcare and Public Health
    m. Information Technology
    n. Nuclear Reactors, Materials, and Waste
    o. Transportation Systems
    p. Water and Wastewater Systems
    q. Unsure

15. [Op] + [FISMA Req] What is the primary website of the impacted entity?
16. [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)**

A. Not applicable **(DESIGN NOTE: Radio button)**
B. Internal tracking number(s) **(DESIGN NOTE: Text box)**

17. [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).
    A. **(DESIGN NOTE: Allow one to many entries. Flag all but first entry as "secondary" addresses of the impacted entity.)**
        1. Not applicable **(DESIGN NOTE: Radio button - Allow to bypass "address info" if not applicable is selected)**
        2. 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)**
        3. Street name and number
        4. City
        5. State
        6. Postal code
        7. Country[21]
    B. 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 option to enter latitude and longitude with guidance on how to use Google Maps to quickly find the coordinates.)**
        1. Not applicable **(DESIGN NOTE: Radio button - Allow to bypass "latitude and longitude info" if not applicable is selected)**
        2. Latitude
        3. Longitude
    C. Has the incident occurred on or involved a movable entity (e.g., ship, aircraft, train)? (Yes/No)
        1. **(DESIGN NOTE: If Yes)** Please describe the entity that was involved in this incident. **(DESIGN NOTE: Open text)**
18. [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),

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

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).**
    a. Type of Identifier(s)
        1. North American Industrial Classification System (NAICS) identifier(s)
            i. Identifier number(s) **(DESIGN NOTE: Repeated for each identifier selected)**
        2. General Services Administration (GSA)-issued Unique Entity Identifier (UEI)
        3. Environmental Protection Agency FacID
        4. What are the Commercial and Government Entity (CAGE) Code(s) for the facility location(s) of the impacted system(s)?
            i. 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.)**
                1. Street name and number
                2. Building number (if applicable)
                3. Suite number (if applicable)
                4. City
                5. State
                6. Postal code
                7. Country[22]
        5. Other [please provide the type of identifier]

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

[RA] Do you work for the affected entity?
A. Not applicable, I am an individual, self-reporting an incident affecting me.
B. Yes
C. Yes, 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:**

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)
A. Is your organization a subsidiary of a larger organization? (Yes/No)

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

1. **(DESIGN NOTE: If Yes)** Provide the name of the larger/parent organization.
2. What is the preferred email address of the parent organization (e.g., soc@organization.gov, soc@organization.com)?
3. [Op] What is the primary website of the parent organization?
4. [Op] Please enter the parent organization'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)**
    a. Not applicable **(DESIGN NOTE: Radio button)**
    b. Internal tracking number(s)

B. Please provide the following information about your organization. (Please answer for your organization and not any parent organization.)
1. What is the preferred email address of your organization?
2. What is the primary website of your organization?
3. [Op] Please enter the your organization'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)**
    a. Not applicable **(DESIGN NOTE: Radio button)**
    b. Internal tracking number(s)

h. Incident Overview

20. [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").)**
21. [RA] When was the incident first detected?
    A. Detection date and time (yyyy-mm-dd HH:MM -<UTC offset>)
22. [RA] Have you performed any incident response activities (e.g., cyber hunt activities) to determine the scope and impact of the incident? (Yes/No)
    A. {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)**

Incident Category Type Determination

23. [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.) (DISPLAY NOTE: Select all that apply)**
    A. Malware [e.g., ransomware, DDOS, etc.]
    B. Human (or technology) errors [e.g., loss of equipment, system misconfiguration, mishandling of sensitive and/or PII documentation, etc.]

C. Hacking [e.g., password cracking, SQL injection, cross-site scripting, 'system' overflows, etc.]
D. Physical actions/destruction [e.g., sabotage, theft, etc.]
E. Environmental factors [e.g., fire, flood, etc.]
F. Social engineering [e.g., phishing, extortion, spam, etc.]
G. Misuse of assets (sometimes called "insider threats') [e.g., privilege abuse, unauthorized hardware/software, etc.]

24. [RA] This incident has led to or resulted in **(DESIGN NOTE: Multi select) (DISPLAY NOTE: Select all that apply)**
A. Classified data "spillage" to unapproved networks
B. Compromised system(s)
C. Destruction of data or systems (not due to ransomware)
D. Destruction of data or systems (via ransomware)
E. Defacement
F. Equipment loss: loss of control of physical equipment not from theft
G. 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[23])
H. Operational technology process control impaired (e.g., physical control processes are manipulated, disabled, or damaged[24])
I. Supply chain customer disruption **(DISPLAY NOTE: The incident involved one of the reporting entity's vendors, with an impact on the reporting entity)**
J. 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)**
K. Unauthorized account access
L. Unauthorized removal of account access (e.g., entity's system administrator's account deleted)
M. Unauthorized information access
N. Unauthorized release of information (virtually via computing systems)[25]

[23] Inhibit Response Function, Tactic TA0107 - ICS | MITRE ATT&CK®
[24] Impair Process Control, Tactic TA0106 - ICS | MITRE ATT&CK®
[25] 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 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.

O. Unauthorized release of information (physically via printed documents or physical media, or orally).[26]
P. Unauthorized use of information
Q. Other [describe]

i. Incident Notifications

25. [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.)**
    A. [CUI]{Conditional} [FISMA Req] **(DESIGN NOTE: If Yes)** Please list the entities you will, or did, report to.
        1. 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)**
            a. Entity Details **(Design Note: Provide check box to allow the reporter to identify if this value is the same as the impacted entity's name. If box is checked, copy the impacted entity's name to this variable)**
                1. Organization Name
                2. [CUI]Point of contact name
                    i. First
                    ii. Last
                3. Email address(es) of Point of Contact
                4. Phone number(s)
            b. Already notified: Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
            c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -<UTC offset>)
            d. Case/incident/report number provided (if applicable)
        2. Inspector general **(DESIGN NOTE: Repeat the following sub entries "a through d" for each notification entity selected, other than the information owner. There can also be more than one entry "a through d" per category, e.g., law enforcement can be local and federal.)**
            a. Entity Details

[26] 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).

1. Organization Name
2. [CUI]Point of contact name
    i. First
    ii. Last
3. Email address(es) of Point of Contact
4. Phone number(s)

b. Already notified: Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -<UTC offset>)
d. Case/incident/report number provided (if applicable)

3. Legal counsel
4. Law enforcement
5. Regulatory agency
6. Privacy officials
7. Security staff
8. System owners
9. Other **(DESIGN NOTE: Repeat the following sub entries a through d for each notification entity selected, other than the information owner. There can also be more than one entry "a through d" per category, e.g., law enforcement can be local and federal.)**

a. Entity Details
    1. Organization Name
    2. [CUI]Point of contact name
        i. First
        ii. Last
    3. Email address(es) of Point of Contact
    4. Phone number(s)
    5. Position/Title
b. Already notified: Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -<UTC offset>)
d. Case/incident/report number provided (if applicable)

B. [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?

1. [If Yes] Which agency? **(DESIGN NOTE: Select from agency list in Appendix 5)**
    a. Entity Details **(Design Note: Provide check box to allow the reporter to identify if this value is the same as the impacted entity's name. If box is checked, copy the impacted entity's name to this variable)**
        1. Organization Name
        2. [CUI]Point of contact name
            i. First
            ii. Last
        3. Email address(es) of Point of Contact
        4. Phone number(s)

b. Already notified: Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -<UTC offset>)
d. Case/incident/report number provided (if applicable)

C. **(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.)**

1. 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.)**
    a. Entity Details **(Design Note: Provide check box to allow the reporter to identify if this value is the same as the impacted entity's name. If box is checked, copy the impacted entity's name to this variable)**
        1. Organization Name
        2. [CUI]Point of contact name
            i. First
            ii. Last
        3. Email address(es) of Point of Contact
        4. Phone number(s)
    b. Already notified: Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
    c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -<UTC offset>)
    d. Case/incident/report number provided (if applicable)
2. Law enforcement **(DESIGN NOTE: Repeat the following sub entries a through d for each notification entity selected, other than the information owner. There can also be more than one entry "a through d" per category, e.g., law enforcement can be local and federal.)**
    a. Entity Details
        1. Organization Name
        2. [CUI]Point of contact name
            i. First
            ii. Last
        3. Email address(es) of Point of Contact
        4. Phone number(s)
    b. Already notified: Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
    c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -<UTC offset>)
    d. Case/incident/report number provided (if applicable)
3. Regulatory agency
4. Other federal agencies
    a. If selected, which agency? **(DESIGN NOTE: Select from agency list in Appendix 5)**

5. Other **(DESIGN NOTE: Repeat the following sub entries a through d for each notification entity selected, other than the information owner. There can also be more than one entry "a through d" per category, e.g., law enforcement can be local and federal.)**
    a. Entity Details
        1. Organization Name
        2. [CUI]Point of contact name
            i. First
            ii. Last
        3. Email address(es) of Point of Contact
        4. Phone number(s)
        5. Position/Title
    b. Already notified: Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
    c. Plan to notify: Date and approximate time (yyyy-mm-dd HH:MM -<UTC offset>)
    d. Case/incident/report number provided (if applicable)

j. Incident: Severity Assessments

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

26. [RA] (**DESIGN NOTE: Logic of all "None" applicable to FISMA reporters – Only. This is an Event-Incident FLAG for FISMA reporters only. If Q26 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[28] 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, if "unsure/None" selected 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.)**
    A. Confidentiality[29] [] imminently; [] actually; [] unsure; [] none **(DESIGN NOTE: Have radio button for all)**

[27] 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

[28] 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}]

[29] "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.]

B. Integrity,[30] [] imminently; [] actually; [] unsure; [] none **(DESIGN NOTE: Have radio button for all)**

C. Availability[31] [] imminently; [] actually; [] unsure; [] none **(DESIGN NOTE: Have radio button for all)**

Violation of Law and Policy

27. [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

A. Violation of law [] imminently; [] actually; [] unsure; [] none **(DESIGN NOTE: Single select have radio button for all.)**

B. Security policies and/or procedures [] imminently; [] actually; [] unsure; [] none **(DESIGN NOTE: Single select have radio button for all.)**

C. Acceptable use policies [] imminently; [] actually; [] unsure; [] none **(DESIGN NOTE: Single select have radio button for all.)**

Incident: High-Level Impacts

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.)

28. [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 "Q29" question, users should see all options from "Q 28 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.)

29. [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: Skip this question if nothing selected in question 28. Display list containing only the options the user**

[30] "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.]

[31] "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)]

selected in Q28. Provide user a "check box" in Q29 so they can indicate which options represent "demonstrable harm.")

Regional Impacts (Local to Global)

30. [Op] + [RR] To the best of your knowledge, describe the extent of the incident's impact on the population/geographic region
    A. Internal/site-specific (Impacts are felt by the impacted entity or a particular facility or site, but not externally)
    B. 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)
    C. State/territory-wide
    D. Regional
    E. Multi-regional
    F. National
    G. Multi-national
    H. Global
    I. Unknown

Breach[32] Severity Impacts

31. [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 personally identifiable information for an other-than-authorized purpose
32. {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)

[32] 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

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 personally identifiable information for an other-than-authorized purpose

(DESIGN NOTE: Following responses for Q31 and Q32, 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)

33. [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 major incident. (DESIGN NOTE: a FISMA major Incident = a significant cyber incident) (DESIGN NOTE: multi select) (DISPLAY NOTE: Select all that apply)**

A. [ ] Unauthorized modification
1. **(DESIGN NOTE: If selected display following:)**
   a. Was this a [ ] potential or [ ] actual occurrence?
   b. Did this occurrence or potential occurrence involve the PII of 100,000 or more people? (Y/N)

B. [ ] Unauthorized deletion
1. **(DESIGN NOTE: If selected display following:)**
   a. Was this a [ ] potential or [ ] actual occurrence?
   b. Did this occurrence or potential occurrence involve the PII of 100,000 or more people? (Y/N)

C. [ ] Unauthorized exfiltration
1. **(DESIGN NOTE: If selected display following:)**
   a. Was this a [ ] potential or [ ] actual occurrence?
   b. Did this occurrence or potential occurrence involve the PII of 100,000 or more people? (Y/N)

D. [ ] Unauthorized access
1. **(DESIGN NOTE: If selected display following:)**
   a. Was this a [ ] potential or [ ] actual occurrence?
   b. Did this occurrence or potential occurrence involve the PII of 100,000 or more people? (Y/N)

34. [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)**

A. **(DESIGN NOTE: If Yes)** Did this change cause the report to (Select one response)
1. [ ] Upgrade to a major incident?

a. Please provide additional context for the change

2. [ ] Downgrade from a major incident?
    a. Please provide additional context for the change
3. [ ] 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)
    a. Please provide additional context

35. [FISMA Req] **(DESIGN NOTE: Only asked of FISMA reporters if the incident has been indicated as a "Major Incident" per thresholds in questions 29 and/or 33.)** Has this incident been reported to Congress? (Yes/No)

Public Health and Safety Impacts

36. [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.)**
    A. No impact – Incident has no impact on public health
    B. 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)
    C. 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)
    D. High impact – Incident has resulted in one or more serious injuries that have required emergency response and/or permanent disabilities
    E. Critical impact – Incident has resulted in one or more deaths
    F. Unknown impact – Reporter does not have information required to assess the impact of the incident on public health
37. [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).")**
    A. No impact – Incident has no impact on public safety
    B. 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)
    C. 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)

D. 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)
E. 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)
F. Unknown impact – Reporter does not have the information required to assess the impact of the incident on public safety

Indirect Impacts

38. [Op] + [RR] To the best of your knowledge, were/are there any indirect (or secondary) impacts to other critical infrastructure sector(s)[33]? (Yes/No)
    A. **(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.")

1. 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)**
    a. Type(s) of Impact: **(DESIGN NOTE: Multi select) (DISPLAY NOTE: Select all that apply)**
        1. Functional impact[34]
        2. Informational impact[35]
        3. Economic impact[36]

[33] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[34] **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
[35] **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
[36] **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

4. Physical impact [37]

b. Subsector list (if available) here: **(DESIGN NOTE: Multi select) (DISPLAY NOTE: Select all that apply)**

1. Type(s) of Impact:
    i. Functional impact
    ii. Informational impact
    iii. Economic impact
    iv. Physical impact
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Financial Services
10. Food and Agriculture
11. Government Facilities
12. Healthcare and Public Health
13. Information Technology
14. Nuclear Reactors, Materials, and Waste
15. Transportation Systems
16. Water and Wastewater Systems
17. Unknown

39. [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)**

A. Functional impact
    1. Not applicable, there is no possibility of indirect functional impact to entities not in a critical infrastructure sector
    2. No impact at this time
    3. Low impact
    4. Moderate impact
    5. High impact
    6. Critical
    7. Unknown

B. Informational impact

[37] **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.

1. Not applicable, there is no possibility of indirect informational impact to entities not in a critical infrastructure sector
2. No impact at this time
3. Low impact
4. Moderate impact
5. High impact
6. Critical
7. Unknown

C. Economic impact
1. Not applicable, there is no possibility of indirect economic impact to entities not in a critical infrastructure sector
2. No impact at this time
3. Low impact
4. Moderate impact
5. High impact
6. Critical
7. Unknown

D. Physical impact
1. Not applicable, there is no possibility of indirect physical impact to entities not in a critical infrastructure sector
2. No impact at this time
3. Low impact
4. Moderate impact
5. High impact
6. Critical
7. Unknown

Impacts Internal to the Entity

Functional Impacts to Entity

40. [Op] + [RR] To the best of your knowledge, what is the current functional impact[38] of this incident?

A. No impact to both non-critical and critical services **(DISPLAY NOTE: Incident has no impact.)**

B. Non-critical services:
1. No impact to non-critical services **(DISPLAY NOTE: Incident has no impact to non-critical services.)**
2. Low impact to non-critical services **(DISPLAY NOTE: Incident has low impact on any business or on delivery to entity customers.)**

[38] **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*

3. Moderate impact to non-critical services **(DISPLAY NOTE: Moderate impact to non-critical services. Some small level of impact to non-critical systems and services.)**
4. High impact to non-critical services **(DISPLAY NOTE: Significant impact to non-critical services. A non-critical service or system has a significant impact.)**
5. Critical impact to non-critical services **(DISPLAY NOTE: Denial of non-critical services. A non-critical system's access is denied, or system's functionality is destroyed.)**
6. Unknown

C. Critical services:

1. No impact to critical services **(DISPLAY NOTE: Incident has no impact to critical services.)**
2. Low impact to critical services **(DISPLAY NOTE: Incident has low impact on any industrial control systems (ICS) or on delivery of critical services to entity customers.)**
3. Moderate impact to critical services[39] **(DISPLAY NOTE: Moderate impact to a critical system or service (e.g., email, active directory).)**
4. High impact to critical services **(DISPLAY NOTE: A critical system has a significant impact (e.g., local administrative account compromise).)**
5. Critical impact to critical services **(DISPLAY NOTE: Denial of critical services/loss of control. A critical system has been rendered unavailable.)**
6. Unknown

41. {Conditional} [Op] + [RR] **(DESIGN NOTE: Only display question if response to "Functional Impact" yields a "Low, Moderate, High, Critical, or Unknown" selection by the reporter for either non-critical or critical services).** Please select (one) the most severe location any observed disruption in your entity's non-critical business or critical system networks from within your environment from this list:

A. Business demilitarized zone (DMZ) (Activity was observed in the business network's demilitarized zone (DMZ))
B. Business network (Activity was observed in the business or corporate network of the entity; these systems would include corporate user workstations, application servers, and other non-core management systems)
C. Business network management (Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores)
D. Critical system DMZ (Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay "jump" boxes into more critical systems.)
E. Critical system management (Activity was observed in high-level critical systems management such as human-machine interfaces in Industrial Control Systems)

[39] **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*

F. Critical systems (Activity was observed in the critical systems that operate critical processes.)
G. Unknown
H. Other [describe] **(DESIGN NOTE: Open Text)**

Informational Impacts to Entity

42. [Op] + [RR] To the best of your knowledge, what is the current informational impact[40] of this incident?
    A. No impact
    B. Low impact
    C. Moderate impact
    D. High impact
    E. Critical impact (unrecoverable)
    F. Unknown

Physical Impacts to Entity

43. [Op] + [RR] To the best of your knowledge, what is the current physical impact[41] of this incident?
    A. No physical impact to both property and systems
    B. Physical impacts to property:
        1. No impact to non-critical and critical property
        2. Low impact to property (**DISPLAY NOTE:** **Damage to non-critical property**)
        3. Moderate impact to property (**DISPLAY NOTE:** **Damage to critical property**[42])
        4. High impact to property (**DISPLAY NOTE:** **Destruction of non-critical property**)
        5. Critical impact to property (**DISPLAY NOTE:** **Destruction of critical property**)
        6. Unknown
    C. Physical impacts to systems:
        1. No impact to non-critical and critical systems
        2. Low impact to systems (**DISPLAY NOTE:** **Damage to non-critical systems**)
        3. Moderate impact to systems (**DISPLAY NOTE:** **Damage to critical systems**)
        4. High impact to systems (**DISPLAY NOTE:** **Destruction of non-critical systems**)
        5. Critical impact to systems (**DISPLAY NOTE:** **Destruction of critical systems**)
        6. Unknown

---

[40] **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*

[41] **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.

[42] **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*

Economic Impacts to Entity

44. [Op] + [RR] To the best of your knowledge, what is the current economic impact[43] 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."[44])**
    A. Incident investigation and forensic analysis
        1. 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)**
    B. Incident response and containment (including direct response, cleanup, and recovery costs)
    C. Lost revenue or productivity
    D. Theft, fraud, and direct financial losses (including any ransomware payments disbursed)
    E. Legal fees and regulatory fines
    F. Victim notification and protection services
    G. Other Losses (e.g., Loss of Intellectual Property)

k. Incident Details

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).[45] 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.)

l. Identification and Detection (I/D) Stage

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:)

[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)**

A. Malware [e.g., ransomware, DDOS, etc.]
B. Human (or Technology) Errors [e.g., loss of equipment, system misconfiguration, mishandling of sensitive and/or PII documentation, etc.]

[43] **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

[44] 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

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

Initial Ransom Demand Details

45. [RC] Please provide the following details about the ransom demand associated with this incident:
    A. [C-15] [Op] + [FISMA Req] Text of ransom demand(s) **(DESIGN NOTE: Open text)**
    B. [C-15] [Op] + [FISMA Req] Screenshot of ransom note(s) or copy of the email(s)
    C. [C-15] [Op] + [FISMA Req] Ransomware variant used (if known)
    D. [C-15] [Op] + [FISMA Req] Amount of ransom demand
    E. [C-15] [Op] + [FISMA Req] Currency type of ransom demand, including virtual currency
    F. [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.)**
    G. [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.)**
    H. [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)
    I. [Op] + [FISMA Req] Does your organization have insurance that covers ransomware demand payments? (Yes/No)
        1. **(DESIGN NOTE: If Yes)** Please provide insurance company details
            a. Name
            b. Email address
                1. Unknown
            c. Website
                1. Unknown
            d. Physical address
                1. Street name and number
                2. Postal code
                3. City
                4. State
                5. Country
            e. Other contact information
            f. 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.)**
                1. Amount
                    i. [ ] Select if primary carrier amount
                    ii. [ ] Ransom coverage only [ ] Total coverage **(DESIGN NOTE: Select one)**
        2. Does the impacted entity plan on seeking, or has it already sought coverage from its insurers for this incident? (Yes/No)

Ransom Payment Details

J. Ransom Payment Details

1. [Op] + [FISMA Req] Was a ransom paid? (Yes/No)
    a. {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.)**
2. {Conditional} [Op] + [FISMA Req] If ransom was paid, provide the following **(DESIGN NOTE: Set Payment Count as 1.)**

(DESIGN NOTE: ==========Ransomware Payment Details==========

a. [CUI] [Op] + [FISMA Req] **Negotiation Details:** Did you use a negotiation agent? (Yes/No), {Conditional} + [Op] + [FISMA Req] **(DESIGN NOTE: If Yes)** Provide
    1. [CUI]Negotiation agent point of contact
        i. [CUI]If person
            1. First
            2. Last
            3. Phone number(s)
            4. Email address(es)
            5. Position/title
        ii. If entity
            1. Name
            2. Email address
                i. Unknown
            3. Website
                i. Unknown
            4. Physical address
                i. Street name and number
                ii. Postal code
                iii. City
                iv. State
                v. Country
            5. 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.)

b. [CUI] [Op] + [FISMA Req] Is the payer an individual or entity? (Select: Individual/entity) **(DESIGN NOTE: Single select)**
    1. [CUI]{Conditional} + [Op] + [FISMA Req] **[Payer]** **(DESIGN NOTE: If Individual)**:

i. First
ii. Last
iii. Phone number(s)
iv. Email address(es)
v. Position/title
vi. Organization

2. [CUI]{Conditional} + [Op] + [FISMA Req] [**Payer**] **(DESIGN NOTE: If Entity)**:
   i. Entity name
   ii. [CUI] Point of contact
      1. First
      2. Last
      3. Phone number(s)
      4. Email address(es)
      5. Position/title
   iii. Entity email address
      1. Unknown
   iv. Website
      1. Unknown
   v. Physical address
      1. Street name and number
      2. Postal code
      3. City
      4. State
      5. Country
   vi. [CUI] Other contact information
3. [CUI] [Op] + [FISMA Req] **[Payer]** Details of transaction 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.)**
   i. Date and time payment was disbursed from the payer making the ransom payment to satisfy the ransom demand
   ii. Currency type (traditional, virtual/digital asset, or other)
      1. Currency
      2. Other, provide description **(DESIGN NOTE: Open text)**
   iii. Amount of payment (may be equal to or different from the actual demand)
      1. In virtual/digital asset
      2. In US dollar value at the time of the transaction

iv. [CUI] For transactions that involved a bank or another type of financial institution (e.g., in facilitating the payment)
    1. Name of bank or financial institution
    2. Address of bank or financial institution
        i. Street name and number
        ii. Postal code
        iii. City
        iv. State
        v. Country
    3. Name(s) on the account
    4. Account number
    5. Routing number
        i. Origin

v. [CUI] If virtual (e.g., crypto) currencies were used:
    1. Service used to
        i. Purchase the currency
        ii. Store the currency
        iii. Transmit the currency
    2. [CUI] Transaction ID (e.g., transaction hash), if known
    3. [CUI] Virtual (crypto) currency address(es)
        i. Payer addresses

vi. Other method of paying the ransom / extortion demands
    1. [CUI] Describe the method

vii. If the transaction occurred at a physical location, please provide
    1. Address of transaction
        i. Geographical point of interest (location)
        ii. Street name and number
        iii. Postal code
        iv. City
        v. State
        vi. Country
    2. Any other physical location characteristics describe here:

c. [CUI] [Op] + [FISMA Req] To the best of your knowledge, is the **recipient** an individual, entity, or group?
Select: [ ]Individual [ ]Entity [ ]Group [ ]Unknown **(DESIGN NOTE: Skip "point of contact" info if "Unknown" selected) (DESIGN NOTE: Single select)**

1. [CUI] [Op] [FISMA Req if selected] [Recipient] **(DESIGN NOTE: If Individual)** Please provide the following information to the extent known:
    i. First
    ii. Middle
    iii. Last
    iv. Suffix
    v. Phone number(s)
    vi. Email address(es)
    vii. Social media information
    viii. Position/title
2. [CUI] [Op] + [FISMA Req if selected] [Recipient] **(DESIGN NOTE: If Entity/Group)** Please provide the following information to the extent known:
    i. Name
    ii. [CUI] Point of contact at entity
        1. First
        2. Middle
        3. Last
        4. Suffix
        5. Phone number(s)
        6. Email address(es)
        7. Position/title
    iii. Entity email address
    iv. Entity social media information
    v. Entity website
    vi. Physical address
        1. Street name
        2. Street number
        3. Postal code
        4. City
        5. State
        6. Country
    vii. Any other contact information describe here:

d. [CUI] [Op] + [FISMA Req if available] [Recipient] Details of transaction 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.)**
    1. Date and time of ransom payment
    2. Currency type (traditional, virtual/digital, or other)
        i. Currency

ii. Other, provide description **(DESIGN NOTE: Open text)**

3. Amount of ransom payment (may be equal to or different from the actual demand)
   i. In virtual/digital asset
   ii. In US dollars
4. [CUI] For transaction(s) that involved a bank or another type of financial institution:
   i. Name of bank or financial institution
   ii. Address of bank or financial institution
      1. Street name and number
      2. Postal code
      3. City
      4. State
      5. Country
   iii. Name(s) on the account
   iv. Account number
   v. Routing number
      1. Destination
5. If virtual (e.g., crypto) currencies were used
   i. Service used to
      1. Purchase the currency
      2. Store the currency
      3. Transmit the currency
   ii. [CUI] Transaction ID (e.g., transaction hash), if known
   iii. [CUI] Virtual (crypto) currency address(es)
      1. Payee addresses

K. [Op] + [FISMA Req] Identifying payment installments
   1. 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**=^^^^^^^^)

Results of Ransom Incident

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

a. [CUI] Describe the type of data stolen or suspected to have been stolen, to the best of your knowledge **(DESIGN NOTE: Open text)**
b. [CUI] Did the threat actors leak any stolen data, to the best of your knowledge? (Yes/No) **(DESIGN NOTE: If Yes)** [describe]
c. [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].

3. [CUI] Describe any additional results of the ransom incident.

M. [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==)**

N. [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)

1. Describe **(DESIGN NOTE: If Yes: Open text)**

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

46. [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, skip over following questions 47, 48, 49, 50).
A. [ ] I'd like to use the offline template **(DESIGN NOTE: If selected, proceed to Q47)**
B. [ ] I'd like to proceed with this report using the online form **(DESIGN NOTE: If selected proceed to Q48)**
47. {Conditional on Q46.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.
A. Download the TTP/IOC template/instructions here: DOWNLOAD TEMPLATE/INSTRUCTIONS
B. Upload the completed TTP/IOC file offline template here: UPLOAD TEMPLATE
1. Select **here** to continue this report and return to upload your offline form later.

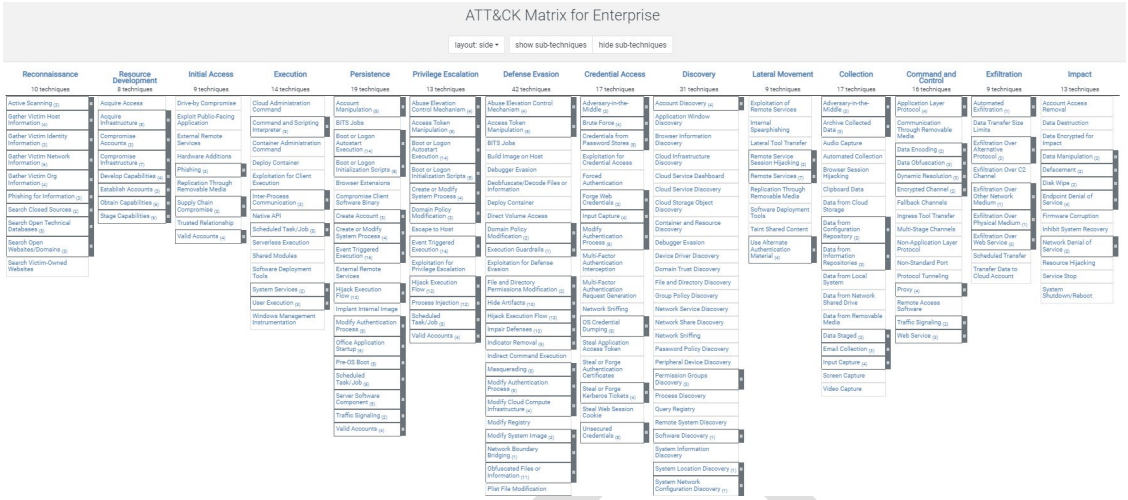
Incident Stage (I/D): Tactics, Techniques and Procedures (TTPs) Observed

48. {Conditional on Q46.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.)**
49. {Conditional}[RC] **(DESIGN NOTE: Question applies only if "Yes" to TTPs to report selection of "Proceed directly in report" to documenting TTP/IOC in Q46.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[46] 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)**
    A. Are you familiar with the MITRE ATT&CK TTP framework? (Yes/No)

    B. Would you like to use CISA's internal tool to help you understand what TTPs you experienced? (Yes/No)
        1. **(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)

    C. **(DESIGN NOTE: If Yes to "familiar with the MITRE ATT&CK" {**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
        1. 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)**

[46] 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.



D. {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)**

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.)

50. [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"

    1. [RC] **(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)**
        a. Upload via copy/paste method
        IOC Relation; Type; Context, Timeline [Start, Stop, Still ongoing (Y/N)]; IOC location observed
            1. Please validate and edit any errors to your IOC(s) here
            2. 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)**
            3. Based on the IOC(s) added to your report, please provide the overall IOC attributes as necessary:

i. Were these IOCs [ ]Attacker, [ ]Benign, [ ]Unknown (Select all that apply) **(DESIGN NOTE: multi select)**

ii. Please provide the timeline of the IOC(s) collected

1. First known time IOC operational in your environment
2. Is the IOC still active in your environment? (Y/N) **(DESIGN NOTE: If No)**
    i. Time IOC ceased operation within your environment

iii. Please select (one) the most severe location any of the IOCs were operating from within your environment from this list:

i. Business demilitarized zone (DMZ) (Activity was observed in the business network's demilitarized zone (DMZ))

ii. Business network (Activity was observed in the business or corporate network of the entity; these systems would include corporate user workstations, application servers, and other non-core management systems)

iii. Business network management (Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores)

iv. Critical system[47] 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.)

v. Critical system management (Activity was observed in high-level critical systems management such as human-machine interfaces in Industrial Control Systems)

[47] **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*

vi. Critical systems (Activity was observed in the critical systems that operate critical processes.)
vii. Unknown
viii. Other [describe] **(DESIGN NOTE: Open Text)**

4. Based on each of the IOCs added to your report, please provide the individual IOC attributes as necessary
   i. Was the IOC [ ]Attacker, [ ]Benign, [ ]Unknown (Select one) **(DESIGN NOTE: Single select)**
   ii. Please provide the timeline of the IOC provided
      1. First known time IOC operational in your environment
      2. Is the IOC still active in your environment? (Y/N) **(DESIGN NOTE: If No)**
         i. Time IOC ceased operation within your environment
   iii. Please indicate any of these areas or locations in your organization's network(s) where you observed the IOC (select all that apply)
      1. Business demilitarized zone (Activity was observed in the business network's demilitarized zone [DMZ])
      2. Business network (Activity was observed in the business or corporate network of the entity; these systems would include corporate user workstations, application servers, and other non-core management systems)
      3. Business network management (Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores)
      4. Critical system[48] 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.)

[48] **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*

5. Critical system management (Activity was observed in high-level critical systems management such as human-machine interfaces in Industrial Control Systems)
6. Critical systems (Activity was observed in the critical systems that operate critical processes.)
7. Unknown
8. Other [describe] **(DESIGN NOTE: Open Text)**

b. 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)**

2. 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.)**

a. 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 =====)**

b. [Op] + [RR] What is the IOC's relation to the incident? (Attacker, Benign, Unknown) **((DESIGN NOTE: Select one)**

c. [C-15] [Op] + [RR] Select type of indicator of compromise **(Select from list:)**:

1. Autonomous System(s) (AS)
2. Domain Name(s)
3. Email Address(es)
4. Email Message(s) **(DESIGN NOTE: Allow option to upload Email Headers separate from Email Body.)**
5. IPv4 Address(es)
6. IPv6 Address (es)
7. Network Traffic
8. URL
9. File System Directory(ies)
10. File Metadata

11. Hash(es)
12. Mutex(es)
13. Software Metadata
14. System Process(es)
15. User Account(s)
16. Windows Registry
17. X.509 Certificate(s)

d. [C-15] + [RA] Please share any relevant context regarding these IOCs **(DESIGN NOTE: Open text)**

e. [Op] + [RR] Please enter your IOC timeline here
   1. First known time IOC operational in your environment
   2. Is the IOC still active in your environment? (Y/N) **(DESIGN NOTE: If No)**
      i. Time IOC ceased operation within your environment

f. [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)

   i. Business demilitarized zone (Activity was observed in the business network's demilitarized zone [DMZ])
   ii. Business network (Activity was observed in the business or corporate network of the entity; these systems would include corporate user workstations, application servers, and other non-core management systems)
   iii. Business network management (Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores)
   iv. 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.)

[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*

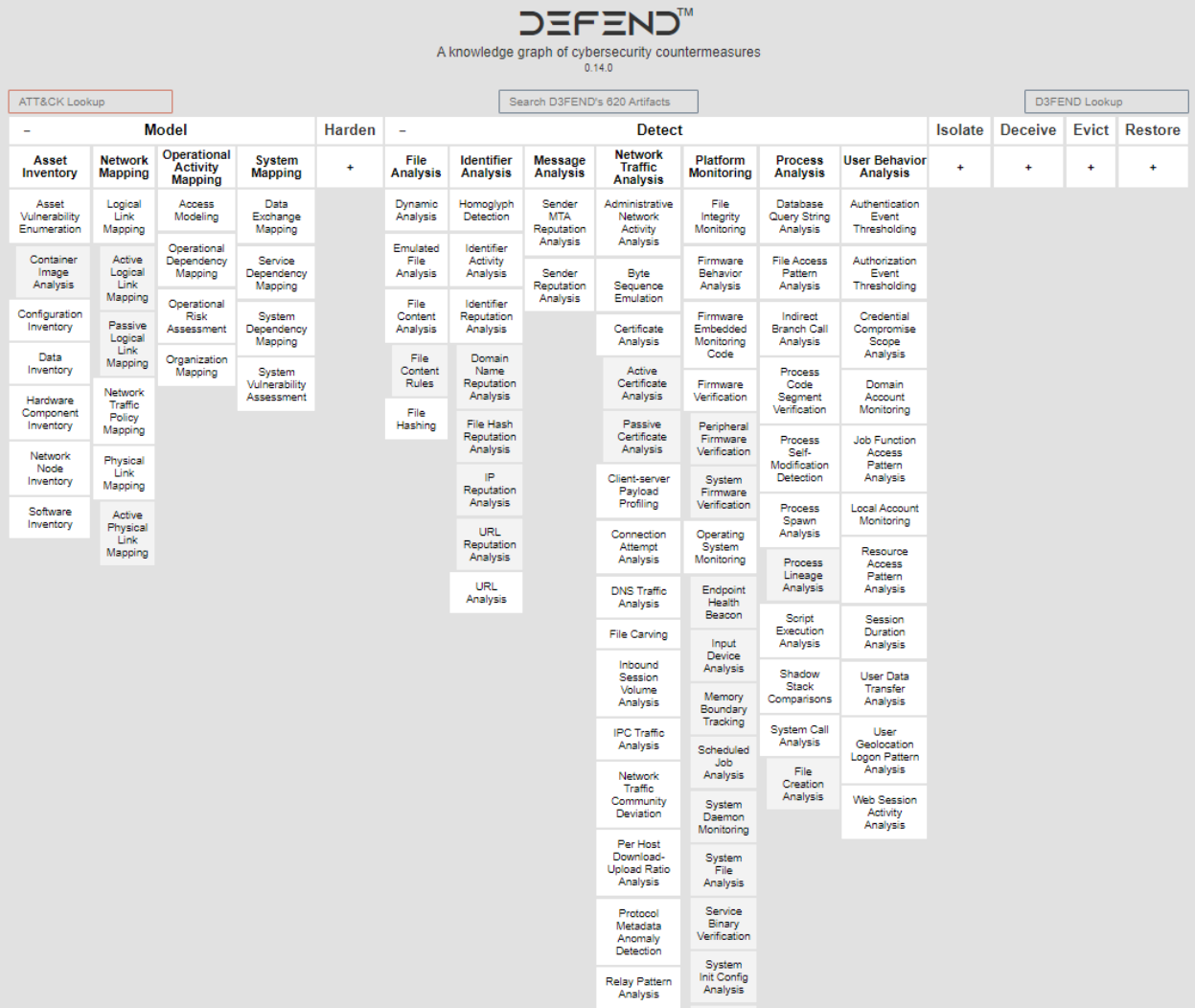
v. Critical system management (Activity was observed in high-level critical systems management such as human-machine interfaces in Industrial Control Systems)
vi. Critical systems (Activity was observed in the critical systems that operate critical processes.)
vii. Unknown
viii. Other [describe] **(DESIGN NOTE: Open Text)**

Indicator of Compromise (IOC) Individual Data Marking

51. [RR except FISMA do not show] 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]

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

52. [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 **(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)**

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

53. [C-15] [RA] Did you detect malicious software (malware) or scripts? (Yes/No)
    A. {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
    B. [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)**

54. [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)**
    A. For each entry, please provide the following
        1. Description
        2. Pattern or rule
        3. Pattern or rule language or technology used (Yara, Snort, SIGMA, etc.)

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

55. [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: See Appendix 1 for options.)

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

Data Sources Used

56. [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)

    [If Yes]Provide the following for each data source

    A. [Op] + [FISMA Req] Report title and number (if applicable)
        1. Name/description of data source (can include author, company providing the data source, or general description)
        2. Link to report/data source (if applicable and available to share)

Attribution

57. [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)

    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)

    A. Threat actor name (could be name of advanced persistent threat [APT] actor, ransomware group, etc.) **(DESIGN NOTE: Open text)**
    B. 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.)**

        1. Name of attribution source(s) **(DESIGN NOTE one to many entries.)**
        2. URL/Web link to validate source material **(DESIGN NOTE: One to many entries.) (DESIGN NOTE: Open text)**
        3. Report title(s) and number(s) (if applicable) **(DESIGN NOTE: One to many entries) (DESIGN NOTE: Open text)**

4. Other details **(DESIGN NOTE: One to many entries.) (DESIGN NOTE: Open text)**

C. What is your level of confidence[50] in your attribution **(DESIGN NOTE: Select one)**
   1. Confirmed by other sources: confirmed by other independent sources; logical in itself; consistent with other information on the subject
   2. Probably true: not confirmed; logical in itself; consistent with other information on the subject
   3. Possibly true: not confirmed; reasonably logical in itself; agrees with some other information on the subject

D. 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)**

m. Assistance

Assistance from CISA

58. [Op] + [RR] Are you interested in receiving incident response assistance from CISA to the extent available? (Yes/No)
59. [Op] + [RR] Are you interested in additional collaboration or information sharing with CISA around this incident to the extent feasible? (Yes/No)

Third Party Assistance

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

Data Sharing and Logging Readiness

61. [OP] + [RR] Are you willing to share the results of third-party analysis with CISA? (Yes/No) **(DESIGN NOTE: Only Display if "Yes" to "third party" question prior.)**
62. [OP] + [RR] Are you willing to share data (such as logs or other technical artifacts) about this incident with CISA? (Yes/No)
    1. {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 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.)**
       a. Identity-based logs for the following

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

1. Identity and credential management
2. Privileged identity and credential management
3. Authentication and authorization
4. User accounts and user account meta-data

b. Network
   1. Email filtering, spam, and phishing logs
   2. Network device infrastructure logs (for devices with multiple interfaces: interface MAC if correlated to the De-NAT IP address)
   3. Network device infrastructure logs (e.g., general logging, access, authorization, and accounting)
   4. Data loss prevention logs
   5. Network traffic (e.g., packet capture) artifacts
   6. Network traffic (e.g., Netflow, Enhanced Netflow, Zeek Logs, etc.) artifacts

c. Host:
   1. Operating systems (e.g., Windows infrastructure and operating systems, MacOS, BSD)
   2. PKI and other multifactor applications and infrastructure
   3. Antivirus and behavior-based malware protection
   4. Other host logs (e.g., operating system, database logs, application logs)

d. Vulnerability
   1. Vulnerability assessments
   2. Penetration test results

e. Mobile
   1. Mobile (phones and tablets) EMM (UEM) / MTD server logs
   2. Mobile (phones and tablets) EMM (UEM) / MTD agent logs

f. Containers:
   1. Container (e.g., supply chain, image, engine (MGT/orchestration, OS, cluster/pod events)

g. Cloud unique data not specified above
   1. Cloud environments (general events and general logging)
   2. System configuration and performance
   3. Virtualization systems

h. Mainframes
   1. Mainframe unique logging not covered above

i. Communications

1. 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.)
2. Notes, transcripts, and audio recordings of any communications with threat actors

j. Financial
   1. 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.)**

k. Forensic images:
   1. Forensic images (e.g., full disk, system, volume etc.) relevant to the incident
   2. Memory images relevant to the incident

l. Malicious code
   1. Malicious code and associated files related to the incident

m. Exfiltrated data
   1. Data and metadata exfiltrated related to the incident **(DISPLAY NOTE: This is not intended to include actual compromised data.)**
   2. Evidence of data and metadata exfiltrated, related to the incident

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

n. Analysis (A) Stage[51]

63. [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.)**
    A. **(DESIGN NOTE: If Yes)** Please provide the date (yyyy-mm-dd) you began the analysis stage
64. [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.)**
    A. **(DESIGN NOTE: If Yes)** Provide date and time (yyyy-mm-dd HH:MM -<UTC offset>) the incident was declared

[51] 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]

Incident Stage (A): Impacted Users and Systems

65. [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.)**
    A. Privileged/system/administrative/service-level IT user quantity impacted **(DESIGN NOTE: Quantity)**
        1. [Op] How are these users impacted (e.g., accounts locked, removed, other)?
    B. Standard IT user quantity impacted **(DESIGN NOTE: Quantity)**
        1. [Op] How are these users impacted (e.g., accounts locked, removed, other)?
66. [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. [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).
        1. **(DESIGN NOTE: If Yes)** Please identify the relevant federal entity category **(DESIGN NOTE: Multi select)**
            a. Federal civilian executive branch (FCEB) - FISMA System (Yes/No)
            b. Intelligence community (Yes/No)
            c. Federal judicial branch (Yes/No)
            d. Federal legislative branch (Yes/No)
            e. DOD system, program, or platform (Yes/No)
    B. {Conditional} **(DESIGN NOTE: Conditional to "Yes" selection to "A.1.a. Federal Civilian Executive Branch (FCEB) - FISMA System (Yes/No)". If Yes)**
        1. [FISMA Req] Please provide the FISMA system name
        2. [FISMA Req] Please select the type of FISMA system
            a. General support system
            b. Major application
            c. Other
                1. Please provide the system type **(DESIGN NOTE: Open text)**
        3. [CUI] [FISMA Req] Contact information of the federal employee identified as the system owner
            a. Name
                1. First
                2. Last

b. Phone number(s)
    1. Unclassified
    2. [Op]Classified
c. Email address(es)
    1. Unclassified
    2. [Op]Classified
d. Position or title

C. [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 (Select all that apply) **(DESIGN NOTE: Multi select)**
    a. [ ]Enterprise networks or systems[52]: Impacted [confirmed] [suspected] (Select one) **(DESIGN NOTE: Single select)**
    b. [ ]Operational technology[53] and industrial control systems: Impacted [confirmed] [suspected] (Select one) **(DESIGN NOTE: Single select)**
    c. [ ]Mobile devices[54]: Impacted [confirmed] [suspected] (Select one) **(DESIGN NOTE: Single select)**

2. Systems type **(DESIGN NOTE: Multi select then quantity entered)**
    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
        4. Media (e.g., backup tapes, disk media (e.g., CDs, DVDs), documents, flash drive or card, hard disk drive, media player, recorder)

[52] 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.

[53] 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))

[54] 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.

5. Mobile phone or smartphone
6. Peripheral (e.g., printer, copier, fax, identity smart card, payment card (such as a magstripe or EMV))
7. Point of sale (POS) terminal
8. Tablet
9. Telephone
10. Voice over Internet Protocol (VoIP) phone
11. Other/unknown **(DESIGN NOTE: Open text)**

b. Server types
    1. Active Directory (AD) Components
        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. Certificate Authority (CA)
    3. Domain Name System (DNS)
    4. Dynamic Host Configuration Protocol (DHCP)
    5. Email
    6. File
    7. File Transfer Protocol (FTP)
    8. Kerberos
    9. Lightweight Directory Access Protocol/Lightweight Directory Access Protocol over Secure Sockets Layer (LDAP/LDAP[S])
    10. Network Time Protocol (NTP)
    11. Print
    12. Remote log(s) (e.g., email, VPN, Syslog, R-Syslog, Syslog-NG)
    13. Remote Shell (RSH)
    14. Security Information and Event Management (SIEM)
    15. Secure Shell (SSH)
    16. TELNET
    17. Virtual Private Network (VPN)
    18. Web
    19. Voice over Internet Protocol (VoIP) Gateways
    20. Authentication, Authorization, and Accounting (AAA) Services (e.g., Radius, Terminal Access Controller Access-Control System [TACACS+])
    21. Operational (OT) and Open-Source Software (OSS) types (e.g., Apache HTTP Server)
    22. Other

i. Please list the additional server type(s) **(DESIGN NOTE: Open text)**

c. Network Devices
   1. Firewalls
      1. Operating systems (OS) (1.i, ii and iii. repeated for each selected)
         i. OS name(s)
         ii. OS version number(s)
         iii. Number impacted of each OS version
   2. Intrusion Detection System (IDS)
   3. Intrusion Protection System (IPS)
   4. Hub
   5. Load Balancers
   6. Proxies
   7. Routers
   8. Switches
   9. Other
      i. Please list the additional network device type(s) **(DESIGN NOTE: Open text)**

d. Identity providers (IdP)
   1. Active Directory
   2. Active Directory Federation Services (ADFS)
   3. Amazon
   4. Azure Active Directory
   5. Facebook
   6. Google Workspace
   7. Lightweight Directory Access Protocol (LDAP)
   8. Login.gov
   9. Ping Federate
   10. OpenID Connect
      i. Provide the name of the provider(s) **(DESIGN NOTE: Open text)**
   11. Okta
   12. Security Assertion Markup Language (SAML)
      i. Provide the name of the provider(s) **(DESIGN NOTE: Open text)**
   13. Other identity providers
      i. Please provide the name of the identity provider(s) **(DESIGN NOTE: Open text)**

3. 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)**

4. Name of system(s) services provided (e.g., active directory, email, web, boundary firewall, key personnel mobile device) **(DESIGN NOTE: Open text)**
5. Physical location(s) of system or group of systems
    a. [ ] Select if same as impacted facility address entered earlier
    b. If not the same address as impacted facility, then please provide address of impacted system(s)
        1. Street name and number
        2. City
        3. State
        4. Postal code
        5. Country
6. 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.)**

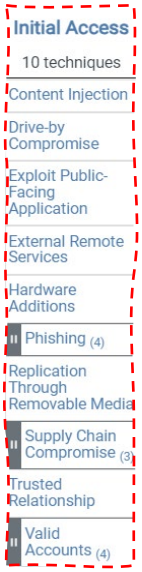
D. [Op] + [RR] Is the system identified as part of the High Value Asset (HVA)[55] Program (Yes/No)
E. [Op] + [RR] Is the impacted system designated as a National Security System[56] (Yes/No)
F. {Conditional}(**DESIGN NOTE: Conditional to "Yes" selection to D. High Value Asset (HVA) Program (Yes/No).)**
    1. What is the HVA Identification Number?
    2. For each HVA listed, what services does it provide?
        a. For each service, what communities does it support? **(DESIGN NOTE: Open text)**
    3. Does this HVA have connections to other HVAs? (Yes/No)
        a. **(DESIGN NOTE: If Yes)** Are these connections internal to the agency, external to the agency, or both? (Internal/External/Both)
        b. **(DESIGN NOTE: If Yes)** Do you know what the other HVAs are? (Yes/No)
            1. **(DESIGN NOTE: If Yes)** Please list the other HVA(s).
                i. For each HVA listed, what services does it provide? **(DESIGN NOTE: Open text)**
                    1. For each service, what communities does it support? **(DESIGN NOTE: Open text)**
            2. Do you have contact information for the other HVA(s)? (Yes/No)
                i. [CUI] **(DESIGN NOTE: If Yes)**
                    1. Name

[55] https://www.cisa.gov/resources-tools/programs/high-value-asset-program-management-office
[56] 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

i. First
ii. Last
2. Phone number(s)
i. Unclassified
ii. [Op]Classified
3. Email address(es)
i. Unclassified
ii. [Op]Classified
4. Position or title
5. Time zone

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

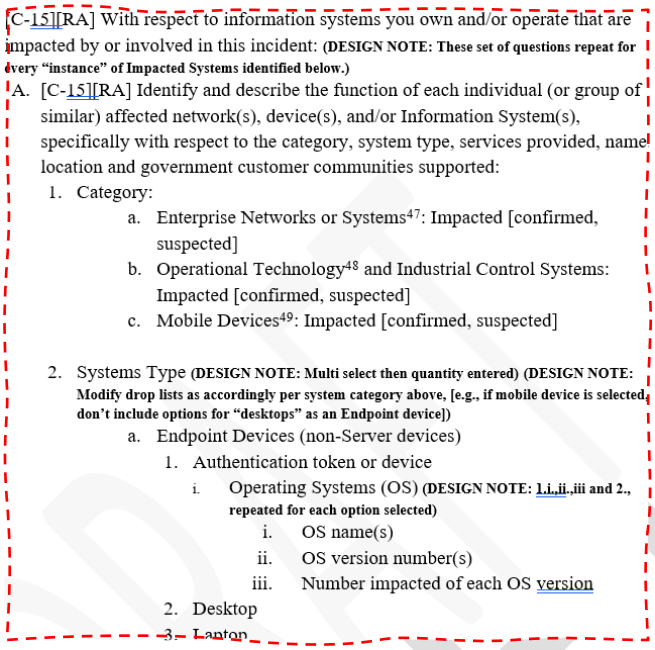
67. {Conditional}[Op] + [RR] **(DESIGN NOTE: Executes if reporter has identified one or more TTPs observed above in the "Initial Access" category in any of the MITRE ATT&CK TTP matrices (example in "red box" to the right), this list is a "Dynamically created" list at time of question determined by which MITRE ATT&CK "Initial Access" TTPs were selected.)** You have observed and identified an "initial access" TTP[57] 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 69.)**



68. {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 any 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 69.)**
69. {Conditional}[Op] + [RR] > [Triggered only if "Yes" from either Q67 or Q68] Please select from your reported initial access observed activity: TTP(s) and provide the technique used to gain the initial access to patient zero.
A. **(DESIGN NOTE: If Yes)** Was the "patient zero" already entered with the rest of the impacted systems? (Yes/No)
1. **(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 in "red box" below) list of "table**

[57] Tactics, Techniques and Procedures (TTP)

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]

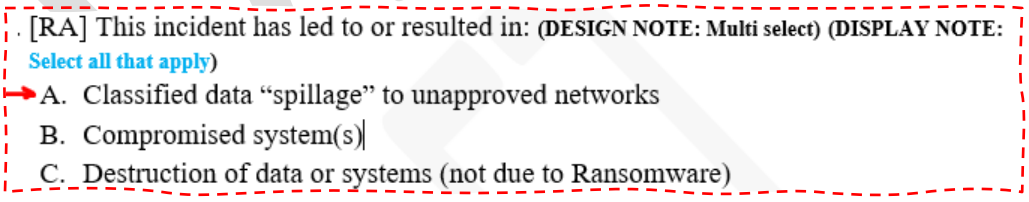
   2. Systems Type **(DESIGN NOTE: Multi select then quantity entered) (DESIGN NOTE: Modify drop lists as accordingly per system category above, [e.g., if mobile device is selected, don't include options for "desktops" as an Endpoint device])**
      a. Endpoint Devices (non-Server devices)
         1. 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

B. [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.
   1. 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.)**

C. When was the date/time of initial access in this incident?
   1. Date and Time (yyyy-mm-dd HH:MM -<UTC offset>)

Incident Stage (A): Detailed Informational Impacts

70. {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:)**


. [RA] This incident has led to or resulted in: **(DESIGN NOTE: Multi select) (DISPLAY NOTE: Select all that apply)**
A. Classified data "spillage" to unapproved networks
B. Compromised system(s)
C. Destruction of data or systems (not due to Ransomware)

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**)

A. What classification guide or source material was used to validate that the information spilled was classified?
B. What was the root cause of the spillage? **(DESIGN NOTE: Open text)**

C. [CUI]Has an appeal or challenge been issued on the spillage of classified information? (Yes/No)
   1. On what date?
   2. [CUI]To whom was the appeal or challenge issued?
   3. Has the appeal been completed? (Yes/No)
   4. Was this appeal accepted or denied? (Accepted/Denied)
      a. If so, on what date was the appeal accepted or denied?

(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[36] of this incident?
A. No impact
B. Low impact
C. Moderate impact
D. High impact
E. Critical impact (unrecoverable)
F. Unknown

71. {Conditional}[RC] Earlier in the form, you selected an informational impact[58] to your entity of **(DESIGN NOTE: Place selected choice of Informational Impact question here, e.g., "High 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?

   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)**
            a. 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)**
               1. How was the <u>suspected</u> information impact discovered? (Select all that apply)
                  i. Some evidence of access but unclear evidence of exfiltration
                  ii. Threat actor has provided inconclusive evidence of information impact (e.g., pictures of file directories)

[58] **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

iii. Other inconclusive evidence of threat actor access/use of the information (please describe) **(DESIGN NOTE: Open text if selected)**
iv. We were informed by an independent third party

2. Was the system where the information was located a critical system[59]? (Yes/No)

b. Communications (e.g., emails, instant messages)
c. Administrative credentials
d. User or other non-administrative credentials
e. Financial
f. Dissemination controlled
   1. Legal
   2. Proprietary
   3. Other personal information
g. Defense information (as the information relates to unclassified cyber threat information/indicators (CTI), export controlled, operational security (OPSEC) and/or information)
   1. Unclassified CTI
   2. Export controlled information
   3. 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)**
         i. Financial **(DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option selected)**
            1. How was the information loss identified? (Select all that apply)
               i. The information was seen outside the authorized system (e.g., darkweb, leaksite, etc.) **(DESIGN NOTE: Flagged as exploited)**

[59] **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*

ii. The information was seen being exfiltrated from the authorized system and/or network **(DESIGN NOTE: Flagged as loss)**
iii. We were informed by an independent third party **(DESIGN NOTE: Flagged as loss)**
iv. Other evidence of threat actor access/use of the information (please describe) **(Design Note: Open Text if selected)**

2. Was the system where the information was located a critical system? (Yes/No)

ii. Dissemination Controlled
1. Legal
2. Proprietary
3. 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)**

iii. Communications **(DESIGN NOTE: 1.i.,ii.,iii and 2., repeated for each option selected)**
1. How was the information loss identified
i. The information was seen outside the authorized system. (e.g., darkweb, leaksite, etc.)
ii. The information was seen being exfiltrated from the authorized system and/or network
iii. We were informed by and independent third party
iv. Other evidence of threat actor access/use of the information (please describe)

2. 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 ask 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)
                A. The information was seen outside the authorized system (e.g., darkweb, leaksite, etc.)
                B. The information was seen being exfiltrated from the authorized system and/or network
                C. We were informed by an independent third party
                D. 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.)
                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)

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

72. {Conditional}[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.

73. [FISMA Req] Did this incident involve a cyber- or non-cyber-related breach of PII? **(DESIGN NOTE: Single-select)**
    A. Cyber-related
    B. Non-cyber related (e.g., personnel information with PII found in a public dumpster)
    C. Both

74. [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)**

Impacted Individuals

75. [FISMA Req] How many individuals' PII was impacted[60]?
76. [FISMA Req] Were affected individuals notified? (Yes/No/Pending)
    A. **(DESIGN NOTE: If Yes or Pending)** How were (or will the) individuals (be) notified? (Select all applicable)
        1. Email
            a. How many individuals were (or will be) notified using this method?
        2. Short message service (SMS)
            a. How many individuals were (or will be) notified using this method?
        3. Verbal
            a. How many individuals were (or will be) notified using this method?
        4. Parcel
            a. How many individuals were (or will be) notified using this method?
        5. Other (Please list the method that was or will be used)
            a. How many individuals were notified using this method?
77. [CUI] [FISMA Req] Were mitigation services in the form of monitoring, insurances and/or counseling provided or offered to affected individuals? (Yes/No)
    A. **(DESIGN NOTE: If Yes)** Which mitigation services have you made available to impacted individuals? (Please select all that apply):
        1. Identity monitoring
        2. Credit monitoring
        3. Identity theft insurance
        4. Full-service identity counseling and remediation services
        5. [CUI] Other (describe)

PII Accessed and/or Impacted

78. [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".)**
    A. *Personally Identifying Numbers* **(DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated for each response selected)**

[60] **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).

1. Full social security number
    a. Provide count
    b. Is this count known or approximate? (Known/Approximate)
    c. Did potential or confirmed access occur? (Potential/Confirmed)
2. Truncated or partial social security number
3. Driver's license number
4. License plate number
5. Drug Enforcement Administration (DEA) registration number
6. File/case identification (ID) number
7. Patient ID number
8. Health plan beneficiary number
9. Student ID number
10. Federal student aid number
11. Passport number
12. Alien registration number
13. Department of Defense (DOD) ID number
14. DOD benefits number
15. Employee Identification Number
16. Professional license number
17. Taxpayer Identification Number
18. Business Taxpayer Identification Number (sole proprietor)
19. Credit/debit card number
20. Business credit card number (sole proprietor)
21. Vehicle Identification Number
22. Business Vehicle Identification Number (sole proprietor)
23. Personal bank account number
24. Business bank account number (sole proprietor)
25. Personal device identifiers or serial numbers
26. Business device identifiers or serial numbers (sole proprietor)
27. Personal mobile number
28. Business mobile number (sole proprietor)
29. Other (please identify)

B. *Biographical Information* **(DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated for each response selected.)**

1. Full name (First, Last, including nicknames)
    a. Provide count
    b. Is this count known or approximate? (Known/Approximate)
    c. Did potential or confirmed access occur? (Potential/Confirmed)
2. Gender
3. Race
4. Date of birth (day, month, year)

5. Ethnicity
6. Nationality
7. Country of birth
8. City or county of birth
9. State of birth
10. Marital status
11. Citizenship
12. Immigration status
13. Religion/religious preference
14. Home address
15. Zip code
16. Home phone or fax number
17. Spouse information
18. Sexual orientation
19. Children information
20. Group/organization membership
21. Military service information
22. Mother's maiden name
23. Business mailing address (sole proprietor)
24. Business phone or fax number (sole proprietor)
25. Global positioning system (GPS)/location data
26. Personal email address
27. Business email address
28. Employment information
29. Personal financial information (including loan information, but not including account or payment card numbers)
30. Business financial information (including loan information, but not including account or payment card numbers)
31. Alias (i.e., username or screenname)
32. Education information
33. Resume or curriculum vitae **(DISPLAY NOTE: If these documents include additional types of PII, e.g., address or SSN, please indicate those fields separately.)**
34. Professional/personal references **(DISPLAY NOTE: If these documents include additional types of PII, e.g., address or SSN, please indicate those fields separately.)**

C. *Biometrics, Distinguishing Features, and Characteristics* **(DESIGN NOTE" Multi select and for sub questions "a., b., c.", repeated for each response selected.)**

1. Fingerprints
    a. Provide count
    b. Is this count known or approximate? (Known/Approximate)
    c. Did potential or confirmed access occur? (Potential/Confirmed)
2. Palm prints

3. Vascular scans
4. Retina/iris scans
5. Dental profile
6. Scars, marks, tattoos
7. Hair color
8. Eye color
9. Height
10. Video recording
11. Photos
12. Voice/audio recording
13. DNA sample or profile
14. Signatures
15. Weight

D. *Medical/Health and Emergency Information* **(DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated for each response selected.)**

1. Physical medical/health information
    a. Provide count
    b. Is this count known or approximate? (Known/Approximate)
    c. Did potential or confirmed access occur? (Potential/Confirmed)
2. Mental health information
3. Disability information
4. Workers' compensation information
5. Patient ID number
6. Emergency contact information

E. *Device Information* **(DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated for each response selected.)**

1. Device settings or preferences (e.g., security level, sharing options, ringtones)
    a. Provide count
    b. Is this count known or approximate? (Known/Approximate)
    c. Did potential or confirmed access occur? (Potential/Confirmed)
2. Cell tower records (i.e., logs, user location, time, etc.)
3. Network communications data

F. *Other Specific Information or File Types* **(DESIGN NOTE: Multi select and for sub questions "a., b., c.", repeated for each response selected.)**

1. Taxpayer information/Tax return information
    a. Provide count
    b. Is this count known or approximate? (Known/Approximate)
    c. Did potential or confirmed access occur? (Potential/Confirmed)
2. Law enforcement information
3. Security clearance/background check information

4. Civil/criminal history information/police record
5. Academic and professional background information
6. Health information
7. Case files
8. Personnel files
9. Credit history information
10. Other
    a. Please provide the other specific information or file type(s)

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

79. [Op] + [RR but **NOT FISMA or FedRAMP reporting**] Please review the "Protect" section of the CISA Cross-Sector Cybersecurity Performance Goals (CPGs).[61] 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)[62] 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.)**
80. {Conditional if Q 79 = Yes} [Op] + [RC] Select the applicable control(s) from the CISA Cybersecurity Performance Goals, "Protect" section[63].
    A. Select from **[DESIGN NOTE: See Appendix 2 for answer options, multi choice select) (DESIGN NOTE: Repeat for each CPG Protect Control selected)**
        1. **(DISPLAY NOTE: Select one)** Was the [ ] failure, [ ] misconfiguration, or [ ]non-implementation of the control due to a published CVE[64](s)?
            a. Yes **(DESIGN Note: The following "CVE" questions are conditional only if the reporter selected "YES" to security controls factoring into the incident)**
                1. What is the CVE(s)?
                (DESIGN NOTE: Multi select for Failed, Misconfigured, and Not implemented) (repeat for each CVE identified)

[61] Cross-Sector Cybersecurity Performance Goals | CISA (https://www.cisa.gov/cross-sector-cybersecurity-performance-goals)
[62] See Appendix 2
[63] See Appendix 2
[64] Common Vulnerabilities and Exposures (CVE) is a program that identifies, defines, and catalogs publicly disclosed cybersecurity vulnerabilities.
https://cve.mitre.org/

b. No
c. Unknown

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

B. 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.)**

81. [**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-Sector Cybersecurity Performance Goals (CPGs) [65] 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.)**
82. {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.

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

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)**
   1. **(DISPLAY NOTE: Select one)** Was the [ ] failure, [ ] misconfiguration, or [ ]non-implementation of the control due to a published CVE[66](s)?
      a. Yes **(DESIGN Note: The following "CVE" questions are conditional only if the reporter selected "YES" to security controls factoring into the incident)**
         1. What was the CVE(s)?
            (DESIGN NOTE: Multi select for Failed, Misconfigured, and Not implemented) (repeat for each CVE identified)
      b. No
      c. Unknown
   2. Does one or more of the observed TTPs reported earlier in this report relate to this selected security control? (Yes/No)
      a. **(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).)**

B. 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.)**

o. Containment (C) Stage [67]

83. [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.)
    A. **(DESIGN NOTE: If Yes)** Provide the date and time (yyyy-mm-dd HH:MM -<UTC offset>) containment activities began
    B. Provide an overview of your containment strategy

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

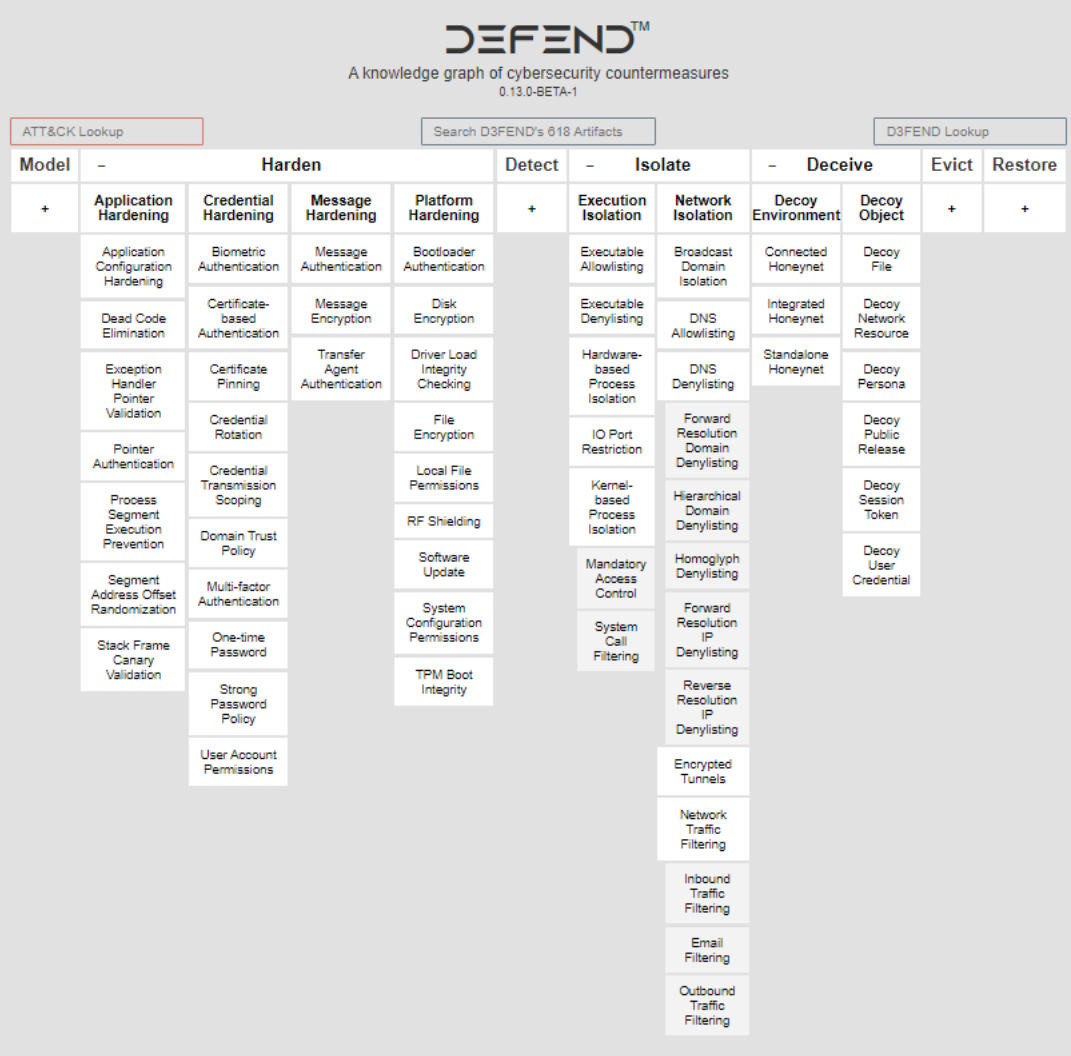
[67] Containment Stage – Stage of the incident life cycle that employs activities before an "incident overwhelms resources or increases damage. Containment provides time for developing a tailored remediation strategy" and can involve many different approaches based on the known severity of the incident 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]

1. If implementation of the containment strategy is complete, was the containment strategy successful? (Y/N)
    a. **(DESIGN NOTE: If No)** Provide details on how your strategy is changing **(DESIGN NOTE: Open text)**

84. [CUI] {Conditional} [Op] + FISMA Req] What specific containment action(s) have been taken? **(DESIGN NOTE: Can be more than one, include options to add)**
    A. Description **(DESIGN NOTE: Open text)**
    B. Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
    C. Has this action been completed? (Yes/No)
        1. **(DESIGN NOTE: If Yes)** Was this action successful? (Yes/No)
            a. **(DESIGN NOTE: If No)** Can you identify why it wasn't successful? **(DESIGN NOTE: Open text)**
            b. [CUI] **(DESIGN NOTE: If No)** Provide details on how your containment action is changing **(DESIGN NOTE: Open text)**
85. [RC] Have you completed containment? (Yes/No)

Incident Stage (C): Countermeasures – Containment

86. [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. (Select all that apply)
    A. Select applicable "containment" counter measures from the MITRE D3FEND list:



B. [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

1. 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)

a. Which tactic did your containment action fall under?

1. Harden

i. Which base technique did your action fall under?

1. Application hardening
2. Credential hardening
3. Message hardening

4. Platform hardening
2. Isolate
   i. Which base technique did your action fall under?
      1. Execution isolation
      2. Network isolation
3. Deceive
   i. Which base technique did your action fall under?
      1. Decoy environment
      2. Decoy object

b. Description **(DESIGN NOTE: Open text)**

2. **(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)**

C. Unknown
D. None

87. [Op] Please provide any additional context for the "containment" countermeasures you have taken **(DESIGN NOTE: Open text)**

p. Eradication Stage [68](E)

88. [CUI] [Op] + [FISMA Req] Have you begun the eradication stage? (Yes/No/Unsure)
    A. [If Yes] Provide the date and time (yyyy-mm-dd HH:MM -<UTC offset>) eradication activities began.
       1. [CUI] {Conditional} [Op] + [FISMA Req] Provide an overview of your eradication strategy **(DESIGN NOTE: Open text)**
       2. {Conditional} [Op] + [FISMA Req] Have you completed the eradication activities? (Yes/No)
          a. **(DESIGN NOTE: If Yes)** Please provide date and time (yyyy-mm-dd HH:MM -<UTC offset>)
          b. **(DESIGN NOTE: If No)** Is the implementation of your eradication strategy complete? (Y/N)
          c. **(DESIGN NOTE: If No)** Was the eradication strategy successful? (Y/N)

[68] 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]

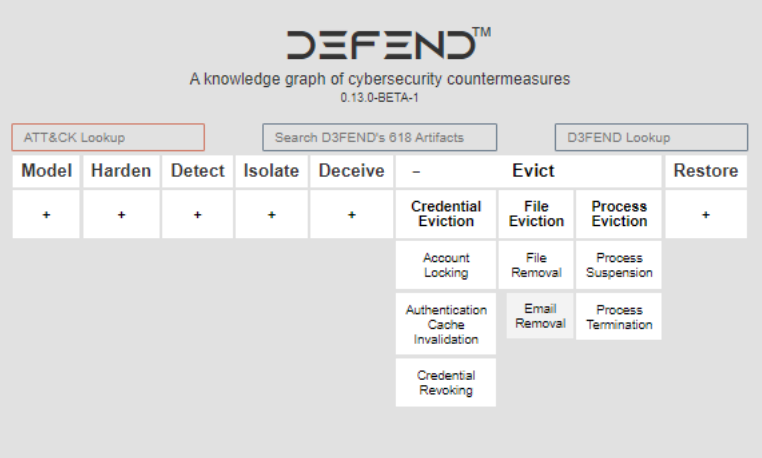
1. **(DESIGN NOTE: If No)** Provide details on how your eradication strategy is changing **(DESIGN NOTE: Open text)**

d. **(DESIGN NOTE: If No)** What specific eradication action(s) have been taken? **(DESIGN NOTE: Can be more than 1, include options to add)**
   1. Description **(DESIGN NOTE: Open text)**
   2. Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
   3. Has this action been completed? (Yes/No)
      i. **(DESIGN NOTE: If Yes)** Was this action successful? (Yes/No)
      ii. **(DESIGN NOTE: If No)** Can you identify why it wasn't successful?
      iii. **(DESIGN NOTE: If No)** Provide details on how your eradication action is changing.

Incident Stage (E): Countermeasures – Eradication

89. [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 (Select all that apply.

A. Select applicable "evict" counter measures from the MITRE D3FEND list:



B. [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.
   1. 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?
      1. Credential eviction
         i. Description

2. File eviction
    i. Description
3. Process eviction
    i. Description

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

C. **(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)**

D. Unknown

E. None

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

q. Recovery (R) Stage [69]

91. [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.)**

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

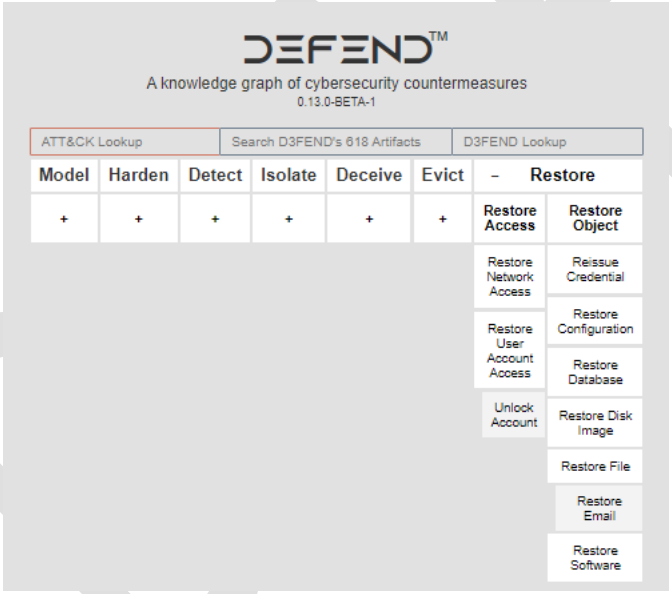
1. Provide the date and time (yyyy-mm-dd HH:MM -<UTC>) Please enter the organization's estimated recovery date and time
    a. Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
2. [Op] + FISMA Req] Describe your recovery strategy **(DESIGN NOTE: open text)**
3. [Op] + [FISMA Req] Have you completed the recovery stage and "accepted" normal operations resumed? (Yes, No)?
    a. **(DESIGN NOTE: If Yes)** Please provide the Date and Time (yyyy-mm-dd HH:MM -<UTC offset>)
4. Was the recovery strategy successful? (Yes/No) **(DESIGN NOTE: If No)**
    a. 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)**

[69] 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]

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

Incident Stage (R): Recovery Actions

93. [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. Select all that apply.
    A. Select applicable "restore" measures from the MITRE D3FEND list:



    B. [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.
        1. 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:

1. Restore access
    i. Description

2. Restore object
    i. Description
2. (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)**

C. Unknown

D. None

94. [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)**

r. Post-Incident (P-I) Stage

95. [Op] + [FISMA Req] Has the incident concluded? (Yes/No)
    (DESIGN NOTE: If Yes) Provide your post incident report/details

A. [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".)**[70]

B. [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.)**
    1. Identification and detection
        a. Which organization could have provided the information? **(DESIGN NOTE: Repeated for each stage selected.)**
    2. Analysis
    3. Containment
    4. Eradication
    5. Recovery
    6. Post-incident

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

C. [Op] + [FISMA Req] Has the impacted organization performed a review of the incident and incident response to identify lessons learned? (Y/N)
    1. **(DESIGN NOTE: If Yes)** Please describe the identified lessons learned in the areas of:
        a. Incident handling processes
        b. Mean time to effective analysis
        c. Mean time to detection
        d. Mean time to response
        e. Mean time to defense
        f. Mean time to reporting
        g. Other

D. [Op] + [FISMA Req] Based on your experience in this incident, please provide recommendations on how CISA can improve the support it provides
    1. What could CISA do differently in future incidents? **(DESIGN NOTE: Open text)**
    2. 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)**
    3. What additional tools or resources would you need to detect, analyze, and mitigate future incidents? **(DESIGN NOTE: Open text)**

s. 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)**

96. [FISMA Req] Has this activity already been reported? (Yes/No)
    A. **(DESIGN NOTE: If Yes)** Provide
        1. Incident report form submission number.
        2. CISA incident tracking number.
97. [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)**
98. [FISMA Req] When did you first detect the activity?
    A. Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
99. [FISMA Req] When did you declare an event?
    A. Date and time (yyyy-mm-dd HH:MM -<UTC offset>)
100. [FISMA Req] Please provide any additional information relevant to the event **(DESIGN NOTE: Open text)**
101. [FISMA Req] Has the entity covered by this event resolved the consequences for the event? (Yes/No)
    A. **(DESIGN NOTE: If Yes)** Provide the date and time when the event was resolved
        1. Recovered as of date/time (yyyy-mm-dd HH:MM -<UTC offset>)
102. [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)**

t. Data Marking Stage

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)

103. [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)
    A. **(DESIGN NOTE: If Yes)** Select question numbers **(DESIGN NOTE: Provide drop-down, multi select).**

Overall Report Data Markings

104. [CUI] [Op] + [RR] The most restrictive marking that has been reported in this incident is X.[71] Is this a valid marking for the entire incident? (Yes/No)
    A. **(DESIGN NOTE: If Yes)** Then the incident marking is X.[72]
    B. **(DESIGN NOTE: If No)** User to enter new marking for the entire incident **(DESIGN NOTE: See Appendix 1 for question options[73])**

u. End of Incident Reporting Questions

v. Appendix 1: Data Marking

Data Marking Options

1. Specific data marking options are as follows
    1. [C-15] Cybersecurity Information Sharing Act of 2015 *commercial, financial, and proprietary*.[74]
    2. [CUI] Controlled unclassified information (CUI).[75]

[71] The default data marking presented here.
[72] The accepted default data marking here.
[73] Option to change default data marking.
[74] 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.
[75] CUI Markings | National Archives

w. Appendix 2: CISA Cybersecurity Performance Goals[76] (Protect) & NIST SP 800-53 References

Protect CISA CPGs & NIST SP 800-53 References

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 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.

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

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 3.1, SR 3.4, SR. 3.8, SR 4.1, SR 4.1, SR 4.2, SR 5.2	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>: 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 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2,	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.

	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 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	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 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, A.12.4.3, A.12.4.4, A.12.7.1	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.
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 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	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) External remote services (T1133, ICS T0822)	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 via proxy or other intermediary, etc.).

x. Appendix 3: Incident Type/Categories

Incident Types involving Malware (based on VERIS with some modifications[77]):

1. Adware
2. Backdoor (enable remote access)
3. Brute force attack
4. Capture data from application or system process
5. Capture data stored on system disk
6. Client-side attack (client-side or browser attack (e.g., redirection, XSS, MitB))
7. Click fraud or Bitcoin mining
8. C2 (command and control)
9. Destroy data (destroy or corrupt stored data)
10. Disable controls (disable or interfere with security controls)
11. DoS (denial of service attack)
12. Downloader (pull updates or other malware)
13. Exploit vulnerability in code (vs misconfiguration or weakness)

[77] Enumerations (verisframework.org)

14. Export data to another site or system
15. Packet sniffer (capture data from network)
16. Password dumper (extract credential hashes)
17. RAM scraper or memory parser (capture data from volatile memory)
18. Ransomware (encrypt or seize stored data)
19. Rootkit (maintain local privileges and stealth)
20. Scan network (scan or footprint network)
21. Spam (send spam)
22. Spyware/Keylogger (spyware, keylogger or form-grabber (capture user input or activity))
23. SQL injection attack
24. Adminware (system or network utilities (e.g., PsTools, Netcat))
25. Worm (propagate to other systems or devices)

Incident Types Involving Hacking (based on VERIS with some modifications [78]):

1. Abuse of functionality
2. Brute force or password guessing attacks
3. Buffer overflow
4. Cache poisoning
5. Session prediction: Credential or session prediction
6. CSRF: Cross-site request forgery
7. XSS: Cross-site scripting
8. Cryptanalysis
9. DoS: Denial of service
10. Foot-printing and fingerprinting
11. Forced browsing or predictable resource location
12. Format string attack
13. Fuzz testing
14. HTTP request smuggling
15. HTTP request splitting
16. Integer overflows
17. LDAP injection
18. Mail command injection
19. MitM: Man-in-the-middle attack
20. Null byte injection
21. Offline cracking: Offline password or key cracking (e.g., rainbow tables, Hashcat, JtR)
22. OS commanding

[78] Enumerations (verisframework.org)

23. Path traversal
24. RFI: Remote file inclusion
25. Reverse engineering
26. Routing detour
27. Session fixation
28. Session replay
29. Soap array abuse
30. Special element injection
31. SQL injection
32. SSI injection
33. URL redirector abuse
34. Use of backdoor or C2
35. Use of stolen creds
36. XML attribute blowup
37. XML entity expansion
38. XML external entities
39. XML injection
40. XPath injection
41. XQuery injection
42. Virtual machine escape

Incident Types Involving Social Engineering (based on VERIS with some modifications [79]):

1. Baiting (planting infected media)
2. Bribery or solicitation
3. Elicitation (subtle extraction of info through conversation)
4. Extortion or blackmail
5. Forgery or counterfeiting (fake hardware, software, documents, etc.)
6. Influence tactics (leveraging authority or obligation, framing, etc.)
7. Scam (online scam or hoax (e.g., scareware, 419 scam, auction fraud))
8. Phishing (or any type of *ishing)
9. Pretexting (dialogue leveraging invented scenario)
10. Propaganda or disinformation
11. Spam (unsolicited or undesired email and advertisements)

Incident Types Involving Misuse of Assets [sometimes called "Insider Threats"] (based on VERIS with some modifications [80]):

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

1. Knowledge abuse: Abuse of private or entrusted knowledge
2. Privilege abuse: Abuse of system access privileges
3. Embezzlement, skimming, and related fraud
4. Data mishandling: Handling of data in an unapproved manner
5. Email misuse: Inappropriate use of email or IM
6. Net misuse: Inappropriate use of network or Web access
7. Illicit content: Storage or distribution of illicit content
8. Unapproved workaround or shortcut
9. Unapproved hardware: Use of unapproved hardware or devices
10. Unapproved software: Use of unapproved software or services

Incident Types Involving Physical Actions (based on VERIS with some modifications [81]):

1. Assault (threats or acts of physical violence)
2. Sabotage (deliberate damaging or disabling)
3. Snooping (sneak about to gain info or access)
4. Surveillance (monitoring and observation)
5. Tampering (alter physical form or function)
6. Theft (taking assets without permission)
7. Wiretapping (Physical tap to comms line)

Incident Types Involving Human (or Technology) Errors (based on VERIS with some modifications [82]):

1. Classification error (classification or labeling error)
2. Data entry error
3. Disposal error
4. Gaffe (social or verbal slip)
5. Loss or misplacement
6. Maintenance error
7. Misconfiguration
8. Misdelivery (direct or deliver to wrong recipient)
9. Omission (something intended, but not done)
10. Physical accidents (e.g., drops, bumps, spills)
11. Capacity shortage (poor capacity planning)
12. Programming error (flaws or bugs in custom code)
13. Publishing error (private info to public doc or site)
14. Malfunction (technical malfunction or glitch)

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

Incident Types Involving Environmental Factors (based on VERIS with some modifications [83]):

1. Deterioration and degradation
2. Earthquake
3. EMI: Electromagnetic interference (EMI)
4. ESD: Electrostatic discharge (ESD)
5. Temperature: Extreme temperature
6. Fire
7. Flood
8. Hazmat: Hazardous material
9. Humidity
10. Hurricane
11. Ice and snow
12. Landslide
13. Lightning
14. Meteorite
15. Particulates: Particulate matter (e.g., dust, smoke)
16. Pathogen
17. Power failure or fluctuation
18. Tornado
19. Tsunami
20. Vermin
21. Volcanic eruption
22. Leak: Water leak
23. Wind

y. Appendix 4: Critical Infrastructure Sectors and Subsectors

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

[83] Enumerations (verisframework.org)

- 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

z. Appendix 5: Federal Agencies and Sub-Agencies

Format of list is as follows:

- Agency
    - Sub-agency

List

- 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

3562 - National Weather Service
3563 - Office of Inspector General
3564 - Office of the Secretary
3565 - Patent and Trademark Office
3566 - Technology Administration
3567 - U.S. Patent and Trademark Office
3568 • Department of Defense (DOD)
3569 - Air Force (USAF)
3570 - American Forces Press Service
3571 - Army (USA)
3572 - Chief Information Officer (CIO)
3573 - Defense Commissary Agency
3574 - Defense Contract and Audit Agency (DCAA)
3575 - Defense Finance and Accounting Service (DFAS)
3576 - Defense Information Systems Agency (DISA)
3577 - Defense Intelligence Agency (DIA)
3578 - Defense Logistics Agency (DLA)
3579 - Defense Security Service
3580 - Defense Technical Information Center (DTIC)
3581 - Joint Chiefs of Staff (JCS)
3582 - Joint Task Force-Global Network Operations (JTF-GNO)
3583 - Marine Corps (USMC)
3584 - Missile Defense Agency (MDA)
3585 - National Guard
3586 - National Security Agency (NSA)
3587 - Navy (USN)
3588 • Department of Education (EDUC)
3589 - Chief Information Officer (CIO)
3590 - Educational Resources Information Center (ERIC)
3591 - Federal Student Aid (FSA)
3592 - National Library of Education (NLE)
3593 - Office of Educational Technology
3594 - Office of General Counsel
3595 - Office of Inspector General
3596 - Office of Intergovernmental and Interagency Affairs
3597 - Office of Legislation and Congressional Affairs
3598 - Office of Management
3599 - Office of Public Affairs
3600 - Office of the Chief Financial Officer
3601 - Office of the Chief Information Officer
3602 - Office of the Secretary
3603 • Department of Energy (DOE)
3604 - 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)

Privacy Act Statement
Incident Reporting Form 2.0
Authority: 44 U.S.C. § 3101 & 3556, and6 U.S.C. § 659(c)(1), (3), (9) authorize the collection of this information.
Purpose: The primary purpose for the collection of this information is to allow the Cybersecurity and Infrastructure Security Agency (CISA) to contact you about your request.
Routine Uses: The information collected may be disclosed as generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act of 1974, as amended. This includes using the information as necessary and authorized by the routine uses published in DHS/ALL-002 - Department of Homeland Security (DHS) Mailing and Other Lists System November 25, 2008, 73 FR 71659.
Disclosure: Some entities are regulatorily or statutorily required to submit incident reports to CISA, and those entities must provide information in this form as required by applicable statute, regulation, or similar mandate. Failure to provide this information may result in inaccurate record keeping of the entity's compliance. For non-mandatory incident reporting, providing this information is voluntary. However, failure to provide this information will prevent CISA from contacting you in the event there are questions about your report.

Paperwork Burden Notice:
The public reporting burden to complete this information collection is estimated at 60 minutes per form response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the collected information. The collection of information is voluntary. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to DHS/ CISA/CSD, 245 Murray Lane, SW, Mail Stop 0640, Arlington, VA 20598-0640 ATTN: PRA [OMB Control No. 1670-00XX].