PRA-Tracked-Changes Document

Prioritized Voluntary Incident Reporting Form Question Set

Table of Contents

a. Labels

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 select they would like certain data markings applied to their responses to the question, and to note where additional language may be displayed to the respondent in the Incident Reporting Portal to assist with question comprehension.

Conditional Logic Markings:

[RA] = Required question for all types of reports

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

[Op] = Optional question

{Conditional} = Additional logic context for conditional questions

Data Markings:

[C-15] = Indicates a CISA 2015 data marking option for non-Federal incident reporting. This is not a default marking for all questions, 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 are not part of the questions that a respondent must answer. Display notes contain additional explanatory content which may assist a respondent with responding to a question. The format for display notes is:

> **(DISPLAY NOTE: Light blue and bolded words should be displayed to the readers.)**
>
> All Endnotes and/or Footnotes will be presented on the form in a method determined during the design process for the best display for the reader. These methods could be a combination of "pop-ups", on form notes, "hover-over" notes, etc.

Design notes are not part of a question that is displayed to respondents and are only 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. The format for design notes is:

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

---

b. Beginning of Voluntary Incident Reporting Questions

(DISPLAY NOTE: Global Disclaimer: Answer the questions to the best of your knowledge at the time of submission.)

(DESIGN NOTE: As needed, provide external resources, definitions, frequently asked questions (FAQ) page, or helper text.)

c. Report Reason

1. [RA] Reason for report: **(DESIGN NOTE: Select one)**
   A. Voluntarily reporting a cyber incident
   B. Satisfying a regulatory, statutory, and/or contractual requirement
      1. Federal Energy Regulatory Commission (FERC)/ North American Electric Reliability Corporation (NERC)
         a. Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security Management Controls) and CIP-008-6 (Cyber Security – Incident Reporting and Response Planning)
      2. Nuclear Regulatory Commission
         a. Cybersecurity event notifications (10 C.F.R 73.77)
      3. Transportation Security Administration (TSA)
         a. 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)
         b. Security Directives or Information Circulars associated with Pipeline Cybersecurity (SD Pipeline 2021-01 series and IC Pipeline 2022-01, including all amendments and successors)
         c. Security Directives or Information Circulars associated with Aviation Cybersecurity (**DESIGN NOTE: Placeholder for aviation citations, details TBD**)
            i. Airport Security Program (ASP)
            ii. Aircraft Operator Standard Security Program (AOSSP)
            iii. Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP)
            iv. Twelve-Five Standard Security Program (TFSSP)
            v. Private Charter Standard Security Program (PCSSP)
            vi. Indirect Air Carrier Standard Security Program (IACSSP)
            vii. Certified Cargo Screening Standard Security Program (CCSSP)
      4. U.S. Coast Guard (USCG)
         a. Suspicious activity, breaches of security, or transportation security incidents (33 C.F.R 101.305)
         b. Actual or threatened cyber incident (33 C.F.R. 6.16-1)
      5. Other (**DISPLAY NOTE: Reporters selecting this option are responsible for confirming that the agency selected and its relevant statute/regulation/contract allow reporting to CISA as a means of compliance with that agency's reporting requirements.**)
         a. [RC] Agency Name [Insert Agency Name]

b. [RC] Statute, regulation, or contract clause [Insert a statutory or regulatory citation or contract clause reference]

d. Report Type

FOR ALL REPORTERS

2. [RA] Report type: **(DESIGN NOTE: Select one)**
   A. Initial Incident Report
   B. Supplemental Report
      1. Enter the previously assigned incident report number:

e. Contact Information

[ ] Information is the same as my registered incident reporting portal profile information

3. [CUI][RA] Reporter contact information.
   A. [CUI] [RA] First Name
   B. [CUI] [RA] Last Name
   C. [CUI] [RA] Phone number
   D. [CUI] [RA] Email address
   E. I am a third party that is expressly authorized to report on the impacted entity's behalf (*e.g.*, a law firm or incident response firm) (Yes/No)
      1. [RC] (Design note: if Yes) What is the name of your third party organization? **(DISPLAY NOTE: Spell out any acronyms.)**

4. Primary Point of Contact (POC) information for the impacted entity. [ ] I am the primary POC for the impacted entity **(Design Note: if selected, populate following information from question 3 to answers 4.a – 4.D and show 4.E. "Job title" to answer. If not selected, show all following questions)**
   A. [CUI] [RA] First Name
   B. [CUI] [RA] Last Name
   C. [CUI] [RA] Phone number
   D. [CUI] [RA] Email address
   E. Job title

f. Impacted Entity Demographics

[ ] Import profile information **(DESIGN NOTE: If reporters have made a profile, provide an option to import following information from their profile. If changes are made to the populated content, provide an option to duplicate changes back into their profile information.)**

[ ] Import profile information for my client. **(DESIGN NOTE: For third-party reporters, provide an option to import information from a specific client profile and a drop-down list connected to their registered profile to select the correct client from list of clients).**

5. [RA] Select the impacted entity type. **(DESIGN NOTE: single select)**

A. Private sector organization (including U.S. Government contractors) **(DESIGN NOTE: skip to question 6.A)**
B. U.S. State, Local, Tribal, or Territorial (SLTT) Government or organization **(DESIGN NOTE: skip to question 6.B)**
C. Foreign government or non-government organization **(DESIGN NOTE: skip to question 6.C)**
D. Civil society organization (*e.g.*, non-governmental organizations, community organizations, academia, media, advocacy groups, etc.) **(DESIGN NOTE: skip to question 6.D)**

6.A {Conditional on selecting Answer 5 A.} [RC] **(DESIGN NOTE: Applies to only "Private sector" selection)** Private Sector Organization – Impacted Entity Demographics

[ ] Information is the same as my registered incident reporting portal profile information **(DESIGN NOTE: If reporters have made a profile, provide an option to import following information from their profile. If changes are made to the populated content, provide an option to duplicate changes back into their profile information.)**

A. [RC] Name of the impacted entity. **(DISPLAY NOTE: Spell out any acronyms.)**
B. [RC] Select the primary critical infrastructure sector and subsector impacted by this reported incident. Add secondary sectors and subsectors, as needed. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list. Primary critical infrastructure sector can only be entered once.)**
    1. Chemical Sector
    2. Commercial Facilities Sector
    3. Communications Sector
    4. Critical Manufacturing Sector
    5. Dams Sector
    6. Defense Industrial Base Sector
    7. Emergency Services Sector
    8. Energy Sector
    9. Financial Services Sector
    10. Food and Agriculture Sector
    11. Government Services and Facilities Sector
    12. Healthcare and Public Health Sector
    13. Information Technology Sector
    14. Nuclear Reactors, Materials, and Waste Sector
    15. Transportation Systems Sector
    16. Water and Wastewater Systems Sector
    17. None

6.B {Conditional on selecting Answer 5 B.} [RC] U.S. State, Local, Tribal, or Territorial (SLTT) Government or Organization – Impacted Entity Demographics

[ ] Information is the same as my registered incident reporting portal profile information **(DESIGN NOTE: If reporters have made a profile, provide an option to import following information from their profile. If changes are made to the populated content, provide an option to duplicate changes back into their profile information.)**

A. Select SLTT Government or Organization type: **(DESIGN NOTE: Single select)**
   1. [ ] U.S. State or Territory Government or Organization
      a. Provide the impacted entity's name **(DISPLAY NOTE: Spell out any acronyms.)**
      b. Select U.S. State or Territory where the impacted entity is located
   2. [ ] Local Government or Organization (**DISPLAY NOTE:** Local administrative division (e.g., city, district, county, township, municipality) and the U.S. state or territory the local administrative division is part of)
      a. Provide the impacted entity's name **(DISPLAY NOTE: Spell out any acronyms.)**
      b. Select the U.S. State or Territory where the impacted entity is located.
   3. [ ] Tribal Government or Organization (**DISPLAY NOTE:** Indicate tribe's name and any U.S. state and/or territories where the tribe is physically located)
      a. Provide the impacted entity's name.
      b. Select the U.S. State(s) or Territory/ies where the impacted entity is located.

B. [RC] Select the primary critical infrastructure sector and subsector that is impacted by the reported incident. Add secondary sectors and subsectors, as needed. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list. Primary critical infrastructure sector can only be entered once.)**
   1. ***Critical Infrastructure list here***

6.C {Conditional on selecting Answer 5 C.} [RC] Foreign Government or Non-Government Organization – Impacted Entity Demographics

[ ] Information is the same as my registered incident reporting portal profile information **(DESIGN NOTE: If reporters have made a profile, provide an option to import following information from their profile. If changes are made to the populated content, provide an option to duplicate changes back into their profile information.)**

A. Select whether the impacted entity is [ ] Foreign Government or [ ] Foreign Non-Government Organization.
B. [RC] Provide the impacted entity's name **(DISPLAY NOTE: Spell out any acronyms.)**
C. Select the country where the impacted entity is located (select from list).
D. Is the impacted entity or third party reporter a Computer Security Incident Response Team (CSIRT)? (Yes/No)
   1. **(DESIGN NOTE: If Yes, show question)** Provide the name of the CSIRT.
E. [RC] Select the primary critical infrastructure sector and subsector as defined by the United States impacted by the reported incident. Add secondary sectors and subsectors, as needed. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list. Primary critical infrastructure sector can only be entered once.)**
   1. ***Critical Infrastructure list here***

6.D {Conditional on selecting Answer 5 D.} [RC] Civil Society Organization – Impacted Entity Demographics

[ ] Information is the same as my registered incident reporting portal profile information **(DESIGN NOTE: If reporters have made a profile, provide an option to import following information from their profile. If changes are made to the populated content, provide an option to duplicate changes back into their profile information.)**

A. [RR] Provide the impacted entity's name **(DISPLAY NOTE: Spell out any acronyms.)**

B. [RC] Select the primary critical infrastructure sector(s) and subsector impacted by the reported incident. **(DESIGN NOTE: See Appendix 4 for complete critical infrastructure sector and subsector list.)**

1. ***Critical Infrastructure list here***

g. Incident Overview

7. [RA] Provide a high-level summary of the incident. **(DISPLAY NOTE: Provide a short "executive summary" of the incident with a narrative of the incident detection. Consider including a description of unauthorized access with substantial loss of confidentiality, integrity, or availability to information and/or information systems. Opportunities to provide more details about this incident will be provided later in this report").**)

h. Incident Type

8. [RA] To the best of your knowledge, select the type(s) of 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, exploit a vulnerability/weakness, 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, exploit a vulnerability/weakness, etc.]
   D. Social engineering (deceit, trickery) [e.g., phishing, extortion, spam, etc.]
   E. Misuse of assets (sometimes called "insider threats") [e.g., privilege abuse, unauthorized hardware/software, etc.]
   F. Other [describe incident type(s)]

i. Incident Stage

Incident Response Life Cycle Stage

9. [RC] Identify the current response life cycle stage(s) of the incident the impacted entity is in or has begun:
   A. [ ] Identification and Detection Stage
   B. [ ] Analysis Stage
   C. [ ] Containment Stage
   D. [ ] Eradication Stage
   E. [ ] Recovery Stage

F. [ ] Fully mitigated and resolved.

j. Incident Severity Assessments and Impacts

Incident: Impacts

Public Health and Safety Impacts

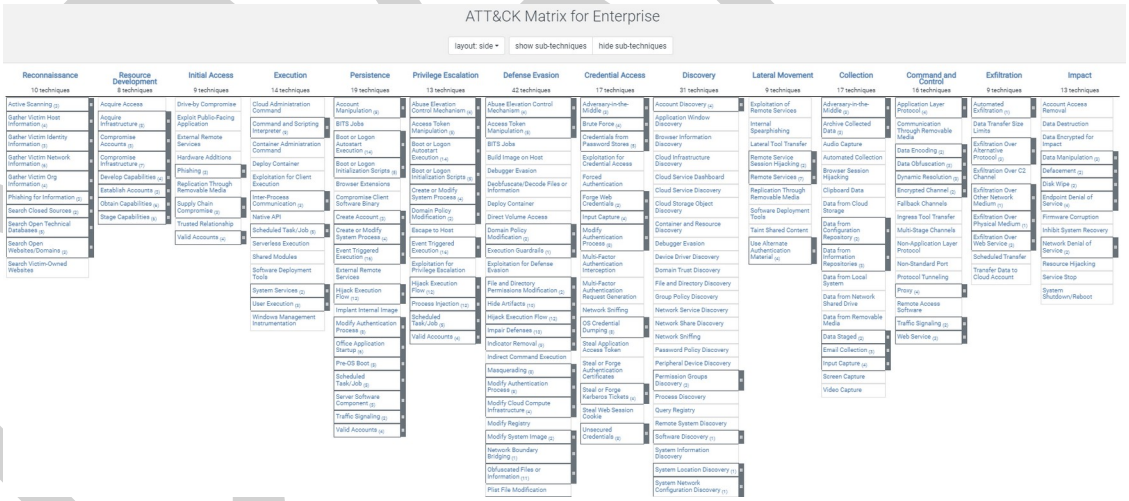
10. [RA] How do the incident's impacts to the impacted entity's operations affect public health and safety?
    A. [ ] No impact/Unknown Impact – Incident has no impact ***or*** the reporter does not have information required to assess the impact of the incident on public health or public safety.
    B. [ ] Low impact –
        1. **Public Health**: 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) and/or
        2. **Public Safety**: Incident has resulted in minimal impact on public safety (e.g., limited, short term disruption (duration under 24 hours) of essential services and/or lifeline resources – phone and internet service, electricity, water).
    C. [ ] Moderate impact –
        1. **Public Health**: Incident has resulted in one or more moderate injuries and/or lasting disabilities that have required emergency response (e.g., easily treated symptoms or hospital diagnostic visits) and/or
        2. **Public Safety**: Incident has resulted in more extensive impact on public safety (e.g., longer-term disruption (duration from 1 – 7 days) of lifeline resources such as phone, internet, electricity, and water; healthcare and shelter impacts; stress on healthcare resources or impeded access to medical records.).
    D. [ ] High impact –
        1. **Public Health:** Incident has resulted in one or more serious injuries that have required emergency response and/or permanent disabilities, and/or
        2. **Public Safety**: Incident has resulted in severe impact on public safety (e.g., evacuation and temporary housing of displaced communities; immediate threats to physical safety of the public; extended disruption (duration lasting more than a week) of essential services; water and air contamination; diversion of patients or cancellation of care from hospitals.)
    E. [ ] Critical impact –
        1. **Public Health**: Incident has resulted in one or more deaths and/or
        2. **Public Safety:** Incident has resulted in a catastrophic impact on public safety (e.g., long-term environmental contamination; cessation of essential services such as law enforcement and healthcare).

Internal Impacts to the Impacted Entity

11. [RA] Select the location of observed access or disruption to any of the following network locations for the reporting entity's information system(s).
    A. [ ] Business or enterprise demilitarized zone (DMZ)
    B. [ ] Business or enterprise network
    C. [ ] Business or enterprise network security management
    D. [ ] Critical system demilitarized zone (DMZ)
    E. [ ] Critical system security management
    F. [ ] Critical systems networks
    G. [ ] Unknown

k. Tactics, Techniques and Procedures (TTPs)

12. [RA] Document the tactics, techniques, and procedures (TTPs) observed. **(DESIGN NOTE: single select)**
    A. Select the type(s) of networks and systems where the TTPs were observed . (Select all that apply.) [ ] Enterprise /Traditional IT; [ ] Operational Technology/Industrial Control Systems; [ ] Mobile Systems
        1. [ ] Submit TTPs using the MITRE ATT&CK framework. **(DISPLAY NOTE: For additional information on MITRE ATT&CK visit [https://attack.mitre.org/matrices/].**
            a. [RC] Select the TTPs observed from the matrix below:



            b. [Op] Provide a description of the TTPs observed. **(DESIGN NOTE: Only show b. if a. is answered)**
        2. [ ] Provide TTPs without using the full MITRE ATT&CK matrix.
            a. Using the type of network(s) that was previously selected, select the TTP category that potentially matches the type of TTP that was observed:

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)		

b. [Op] Provide a description of the TTPs observed in the network category(ies) that were selected **(DESIGN NOTE: Only show b. if a. is answered.**

3. [ ] There are no TTPs to report at this time **(DESIGN NOTE: Skip TTP questions, go to next question) (DISPLAY NOTE: When, during the investigation, new information is discovered about TTPs , return to this section.)**

l. Indicators of Compromise (IOCs)

13. [C-15] [RA] Document Indicators of Compromise (IOCs) observed that describe the reported incident and/or TTPs:
    A. [ ] There are no IOCs to report at this time **(DESIGN NOTE: if selected, skip to next question)**
    B. [ ] There are IOCs to report at this time
        1. [ ] Select if the information contained in this submission should be considered commercial, financial, or proprietary under the Cybersecurity Information Sharing Act of 2015.
        2. Select the indicator type **(DESIGN NOTE: see Appendix 1 for drop down list information) (DESIGN NOTE: Allow for reporter to add more than one IOC as necessary, i.e. a "+ Add IOC here" button)**
        3. [RC]Provide the IOC in the text box or upload screenshots (*e.g.*, Insert the IP addresses, domain names, file hashes, etc for the "Indicator Type" selected).
        4. [RC] **(DESIGN NOTE: Do not present this question if no TTPs are previously reported)** Associate the IOC(s) provided with any previously reported TTP(s). [ ] IOCs are unable to map to previously reported TTPs shown below. **(DESIGN NOTE: if box checked here, skip to "Provide indicator of compromise context…" DISPLAY NOTE: When, during the investigation, the impacted entity discovers knowledge about TTPs contributing to the incident and have documented them, 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 TTP(s).)**

5. [RC] Provide contextual information about the IOC even if unable, at this time, to map the IOC to a TTP

Indicators of Compromise (IOCs): Detection Methods

14. [Op] Document the IOC detection method(s) used to find any reported IOC.
    A. [ ] I don't have any IOC detection methods to report at this time
    B. The IOC detection method(s) used include: **(DESIGN NOTE: Multi select drop down list)**
        1. Actor disclosure
        2. Antivirus
        3. Audit
        4. Customer
        5. Data loss prevention
        6. Emergency response team
        7. Financial audit
        8. Found documents
        9. Fraud detection
        10. Fraud detection by 3rd party
        11. Host-based Intrusion Detection System (HIDS)
        12. Incident response
        13. Incident response by 3rd Party
        14. Infrastructure monitoring
        15. IT review
        16. Law enforcement
        17. Log review
        18. Network-based Intrusion Detection System (NIDS)
        19. Offboarding
        20. Reported by employee
        21. Security alarm
        22. Security researcher
        23. Suspicious traffic
        24. Unrelated 3rd party
        25. Other

Detection Logics/Analytics

15. [C-15] [Op] Were any signatures or other detection analytics in place to identify and/or detect the threat activity ? (Yes/No)
    A. {Conditional} [Op] For each signature or detection analytic that was in place, provide the following:
        1. [ ] Select if the information contained in this submission should be considered commercial, financial, or proprietary under the Cybersecurity Information Sharing Act of 2015.

2. Description
3. Pattern or rule
4. Pattern or rule language or technology used, by selecting from the following: **(DESIGN NOTE: Provide comprehensive drop list for reporter to choose from, i.e. Yara, Snort, SIGMA, etc. and "other")**

m. Impacted User Accounts and Systems

16. [Op] Identify the type and quantity of user accounts that provide access to the organization's information system or network impacted. **(DESIGN NOTE: Multi select then quantity entered.)**
    A. [ ] Privileged/system/administrative/service-level information system or network account **(DISPLAY NOTE: Enter quantity impacted [ ])**
        1. [Op] How were these account(s) impacted, select from the following: **(DESIGN NOTE: Multi-select)**
            a. [ ] Unauthorized Disclosure
            b. [ ] Unauthorized Acquisition
            c. [ ] Loss of Control
            d. [ ] Exfiltrated
            e. [ ] Modified
            f. [ ] Deleted
            g. [ ] Compromised in some other manner
    B. [ ] Standard information system or network account **(DISPLAY NOTE: Enter quantity impacted [ ])**
        1. [Op] How were these account(s) impacted, select from the following: **(DESIGN NOTE: Multi-select)**
            a. [ ] Unauthorized Disclosure
            b. [ ] Unauthorized Acquisition
            c. [ ] Loss of Control
            d. [ ] Exfiltrated
            e. [ ] Modified
            f. [ ] Deleted
            g. [ ] Compromised in some other manner
17. [RA] Identify and describe each impacted network type, device, and/or information technology system owned or operated by the impacted entity. [ ] Unknown at this time. **(DESIGN NOTE: Skip to next question if this check box selected.) (DESIGN NOTE: Allow for one-to-many entries of impacted systems)**
    A. [RA] Network Type **(DESIGN NOTE: Single select per impacted system entry)**
        a. [ ] Enterprise networks or systems
        b. [ ] Operational technology and industrial control systems
        c. [ ] Mobile devices
    B. [RA] Systems Type & Services Provided **(DESIGN NOTE: Single select per impacted system entry)**
        a. **[Type]** Endpoint devices (non-server devices) **(DESIGN NOTE: See Appendix 1 for drop down list information)**

b. **[Type]** Servers **(DESIGN NOTE: See Appendix 1 for drop down list information)**

c. **[Type]** Network Devices **(DESIGN NOTE: See Appendix 1 for drop down list information)**

d. **[Type]** Identity providers (IdP) **(DESIGN NOTE: See Appendix 1 for drop down list information)**

C. (**DESIGN NOTE: Only show this Patient Zero question if there was an Initial Access TTP previously entered in the TTP question)** [RA] Select here [ ] if this "Impacted System" entry is considered as the "patient zero" impacted system.

1. [RC] When was the date and time of initial access for this incident? [ ] Unknown at this time.
2. [Op] Associate "patient zero" with the appropriate TTP(s) reported for this incident. [ ] The "patient zero" TTP is unknown at this time.

n. Vulnerabilities

18. [RA] What vulnerabilities were exploited to perpetrate the incident? Provide the associated Common Vulnerabilities and Exposures Identifiers (CVE-ID). [ ] Unknown at this time. **(DISPLAY NOTE: Do not include the letters "CVE" as a prefix, enter only the CVE number (e.g., 2014-7654321) (DESIGN NOTE: Allow for more than one entry and look up the CVE in database and display to reporter.)**

o. Detailed Information Impacts

19. [RA] Did the impacted entity experience an informational impact as a result of the incident? [ ] Yes; [ ] No; [ ] Unknown at this time (select one)

A. [ ] Personally Identifiable Information (PII)/Privacy Data Breach,-

1. Identify the type of Privacy Data Breach that occurred involving access to PII Choose all that apply: **(DESIGN NOTE: Multi select)**
    a. [ ] Unauthorized Disclosure
    b. [ ] Unauthorized Acquisition
    c. [ ] Loss of Control
    d. [ ] Exfiltrated
    e. [ ] Modified
    f. [ ] Deleted
    g. [ ] Compromised in some other manner
    h. [ ] Any occurrence where a person other than an authorized user accesses PII
    i. [ ] Any occurrence where an authorized user accesses PII for an other than authorized purpose
2. Identify the type(s) of PII involved in this privacy data breach. Choose all that apply: **(DESIGN NOTE: Multi-select)**
    a. [ ] Unique individual identifiers **(DESIGN NOTE: Hover over (DISPLAY NOTE: e.g. social security number, passport number, etc.)**
    b. [ ] Personal information **(DESIGN NOTE: Hover over (DISPLAY NOTE: e.g., home address, phone number, etc.)**

c. [ ] Financial information **(DESIGN NOTE: Hover over (DISPLAY NOTE: e.g., bank account numbers, credit card numbers, etc.)**
d. [ ] Medical or Health information **(DESIGN NOTE: Hover over DISPLAY NOTE: e.g. health records, lab test results, etc.)**

B. [ ] Financial (non-PII) Information
C. [ ] Attorney/Client Privileged Information
D. [ ] Proprietary Business Information Compromise **(DESIGN NOTE: Multi-select)**
   1. [ ] Trade Secrets
   2. [ ] Customer Lists
   3. [ ] Research and development information
   4. [ ] Other
E. [ ] Core Credentials **(DESIGN NOTE: Multi-select)**
   1. [ ] Non-administrative credentials
   2. [ ] Administrative credentials
F. [ ] Destruction of Non-Critical System
G. [ ] Critical Systems Data Compromise
H. [ ] Destruction of Critical System
I. [ ] Defense information (as the information relates to unclassified cyber threat information/indicators (CTI), export-controlled information, and/or OPSEC information) **(DESIGN NOTE: Multi-select)**
   1. [ ] CTI
   2. [ ] Export-controlled information
   3. [ ] OPSEC information
J. [ ] Unclassified communications
K. [ ] Classified communications
L. [ ] Other

p. Attribution

20. [Op] If the impacted entity has attributed this incident, provide the following:.
    A. If the incident is not attributed, select N/A here [ ].
    B. The name of the threat actor.
    C. Any identifying information for the threat actor.

q. Malware Artifacts Conditional Question

21. {Conditional} [RC] A cyber incident type reported earlier in this form included malware. Did the impacted entity detect malicious software (malware) or scripts? (Yes/No)
    A. {Conditional} [Op] If available, upload a sample of the malware here. **(DESIGN NOTE: Provide user a file upload button. Provide a notice to users that all uploaded malware will be submitted into CISA's Malware Next Generation system.)**
    B. {Conditional} [Op] Describe the malware and any additional context regarding the malware.

r. Optional Additional Information

22. [Op] Provide any optional additional information relevant to describe or understand the incident, such as: **(DESIGN NOTE: provide droplist options below and a capability to upload and an open text description for each category selected)**
    A. Third-Party Analysis Results
    B. Data such as Logs or other Technical Artifacts
    C. External data sources used to discover, or aid in discovering, the reported incident (including report titles, descriptions, and links)
    D. Attribution details or information relevant to aid in attribution
    E. Observations for PII breach (note: DO NOT include samples of actual PII in this response)
    F. Containment strategy details (including specific containment actions taken, if the containment strategy was successful, and how it has changed)
    G. Eradication strategy details (including specific eradication actions taken, if the eradication strategy was successful, and how it has changed)
    H. Recovery strategy details (including specific recovery actions taken, if the recovery strategy was successful, and how it has changed)
    I. Post-Incident Details or After Action/Lesson Learned
    J. Other (any other relevant information to describe or understand the incident)