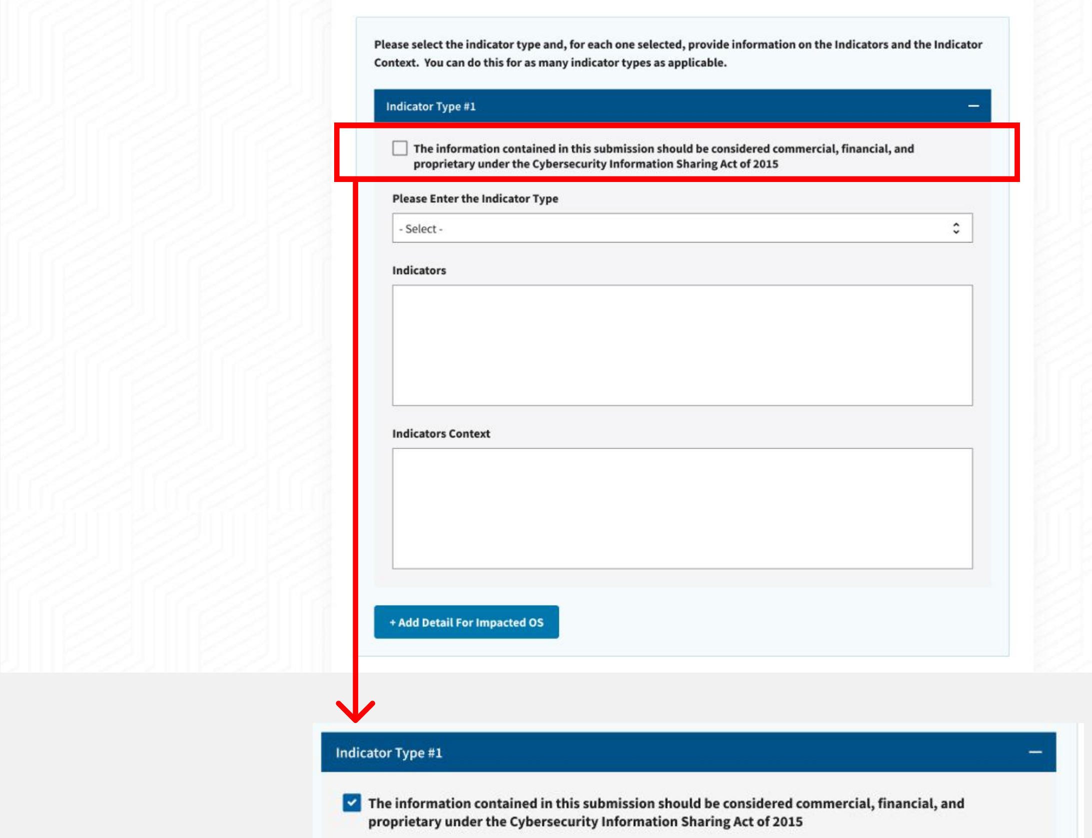
Indicator Type Checkbox



Please select the indicator type and, for each one selected, provide information on the Indicators and the Indicator Context. You can do this for as many indicator types as applicable.

Indicator Type #1 —

□ The information contained in this submission should be considered commercial, financial, and proprietary under the Cybersecurity Information Sharing Act of 2015

Please Enter the Indicator Type

- Select -

Indicators

Indicators Context

Indicator Type #1 —

☑ The information contained in this submission should be considered commercial, financial, and proprietary under the Cybersecurity Information Sharing Act of 2015

Requirements

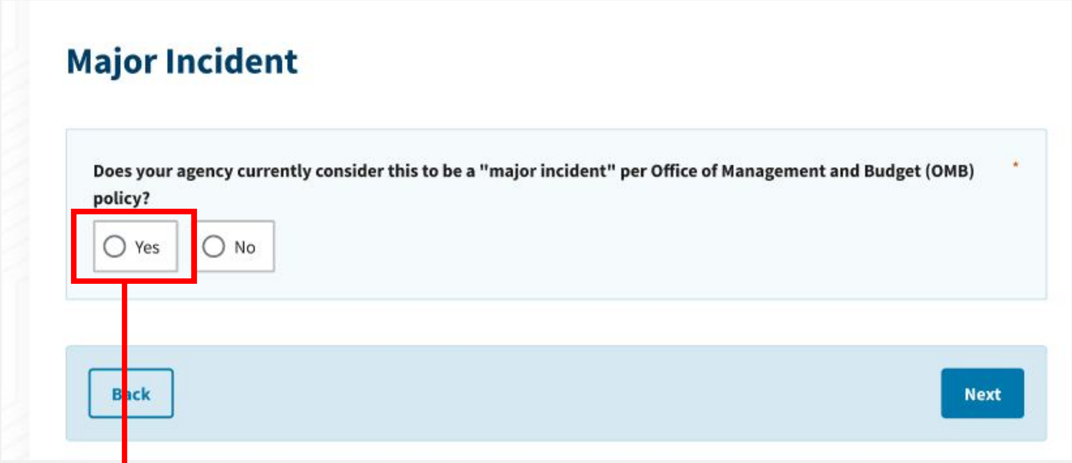
On the impact details section each Indicator Type should have a checkbox that allows users to report whether that particular indicator has sensitive data with the following text after the checkbox:

“The information contained in this submission should be considered commercial, financial, and proprietary under the Cybersecurity Information Sharing Act of 2015 ”

Notes

- This new checkbox is located within the Indicator type question under **“Impact Details”**
- If the user indicates **“United States Federal Government”** under the Organization Details, this check box **WILL NOT** appear
- This checkbox will be asked for each Indicator type the user adds.

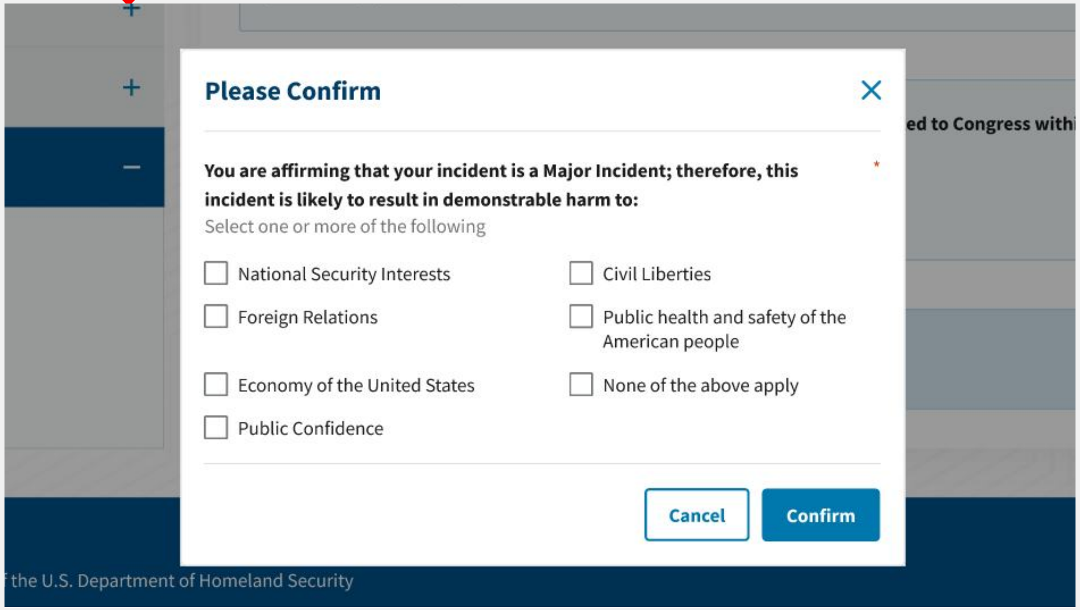
Major Incident



Major Incident

Does your agency currently consider this to be a "major incident" per Office of Management and Budget (OMB) policy? *

○ Yes ○ No



Please Confirm

You are affirming that your incident is a Major Incident; therefore, this incident is likely to result in demonstrable harm to: *

Select one or more of the following

- □ National Security Interests
- □ Foreign Relations
- □ Economy of the United States
- □ Public Confidence
- □ Civil Liberties
- □ Public health and safety of the American people
- □ None of the above apply

Notes

- These questions will determine if a Fed Gov submission constitutes as a major incident.
- Located under **"Impact Details"**
- This question will only appear if the user indicates "United States Federal Government" under the Organization Details

Flow

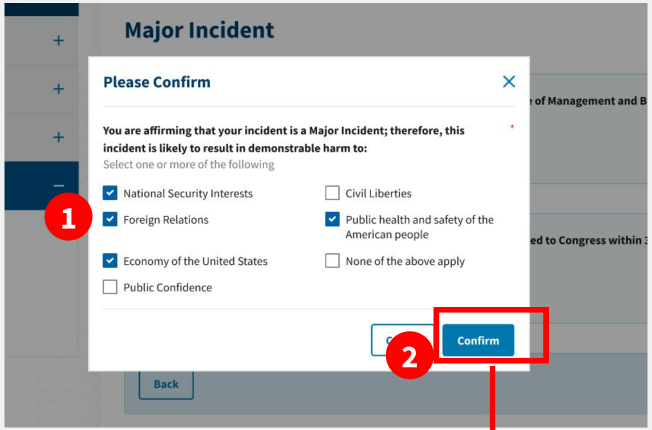
If the user selects "**No**", no follow up questions will be asked.

If the user selects "**Yes**" a popup will appear with the check boxes as seen in the screenshot.

Note: There are three conditions that will confirm the incident is a major incident.

If any of the three following conditions are true, then the incident is confirmed as a major incident. All 3 options do not have to be true, just one or more.

Major Incident - Condition 1



Major Incident

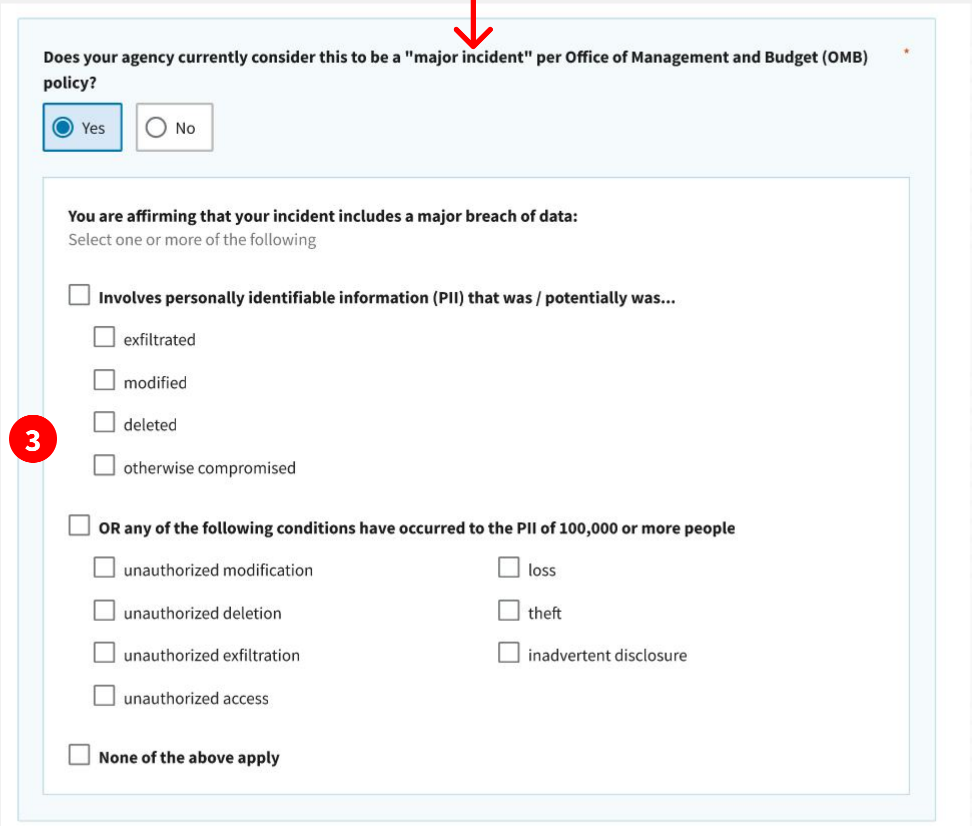
Please Confirm

You are affirming that your incident is a Major Incident; therefore, this incident is likely to result in demonstrable harm to: *

Select one or more of the following

☑ National Security Interests
☐ Civil Liberties
☑ Foreign Relations
☑ Public health and safety of the American people
☑ Economy of the United States
☐ None of the above apply
☐ Public Confidence

Confirm



Does your agency currently consider this to be a "major incident" per Office of Management and Budget (OMB) policy? *

● Yes ○ No

You are affirming that your incident includes a major breach of data:

Select one or more of the following

☐ Involves personally identifiable information (PII) that was / potentially was...

☐ exfiltrated
☐ modified
☐ deleted
☐ otherwise compromised

☐ OR any of the following conditions have occurred to the PII of 100,000 or more people

☐ unauthorized modification
☐ unauthorized deletion
☐ unauthorized exfiltration
☐ unauthorized access
☐ loss
☐ theft
☐ inadvertent disclosure

☐ None of the above apply

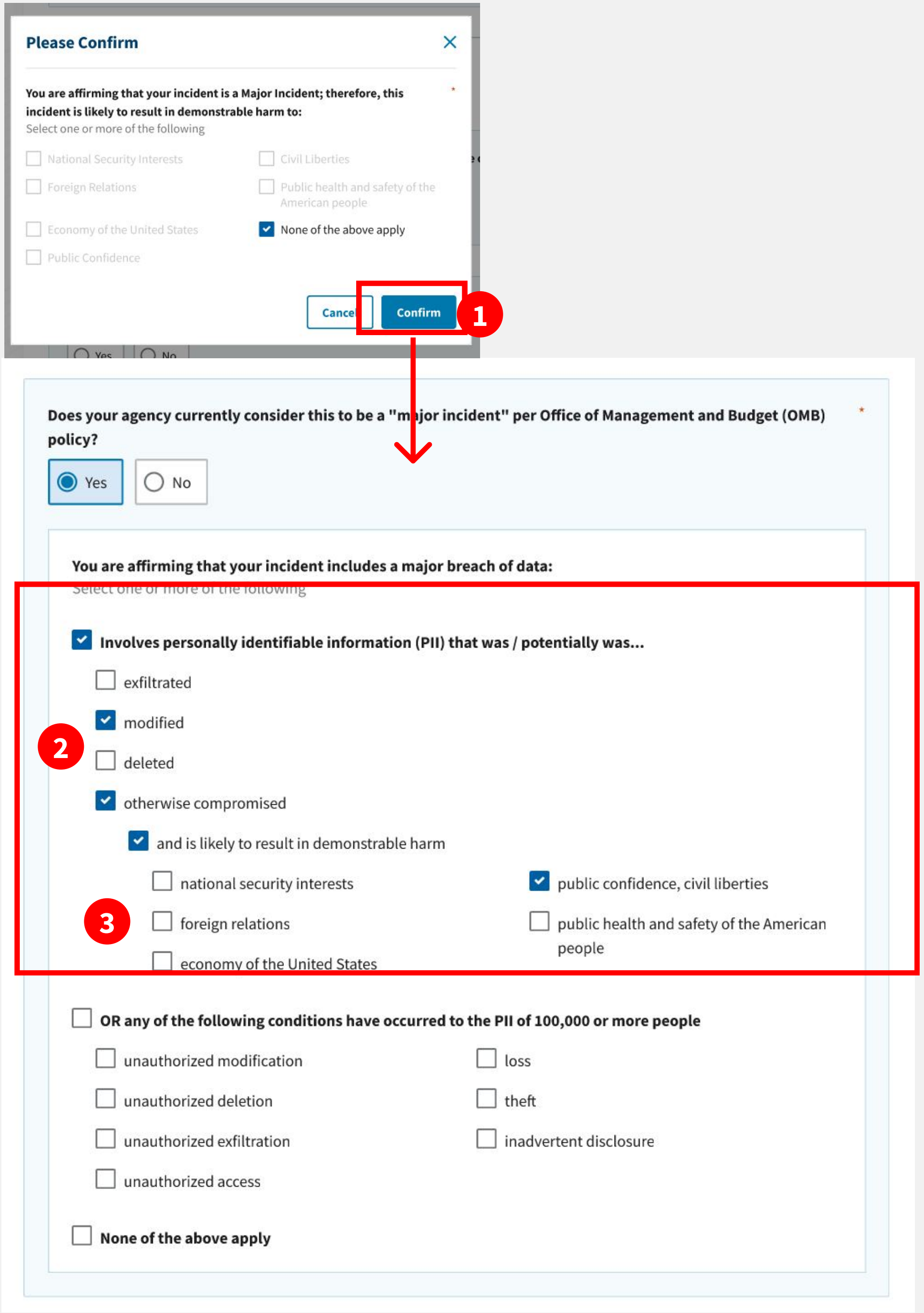
Condition 1 Flow

1. If the user **selects any** option other than "none of the above apply" within the pop-up, it will be **classified as a major incident**, regardless of their responses to the follow up questions.

2. Once the user selects their check boxes and clicks confirm, the Major Incident question will be marked as **YES**, and new fields will appear below.

3. Users will then proceed to check all applicable boxes to the follow up questions.

Major Incident - Condition 2



Please Confirm ✕

You are affirming that your incident is a Major Incident; therefore, this incident is likely to result in demonstrable harm to: *

Select one or more of the following

□ National Security Interests	□ Civil Liberties
□ Foreign Relations	□ Public health and safety of the American people
□ Economy of the United States	☑ None of the above apply
□ Public Confidence	

Does your agency currently consider this to be a "major incident" per Office of Management and Budget (OMB) policy? *

● Yes ○ No

You are affirming that your incident includes a major breach of data:

Select one or more of the following

☑ **Involves personally identifiable information (PII) that was / potentially was...**

- □ exfiltrated
- ☑ modified
- □ deleted
- ☑ otherwise compromised
  - ☑ and is likely to result in demonstrable harm
    - □ national security interests
    - □ foreign relations
    - □ economy of the United States
    - ☑ public confidence, civil liberties
    - □ public health and safety of the American people

□ **OR any of the following conditions have occurred to the PII of 100,000 or more people**

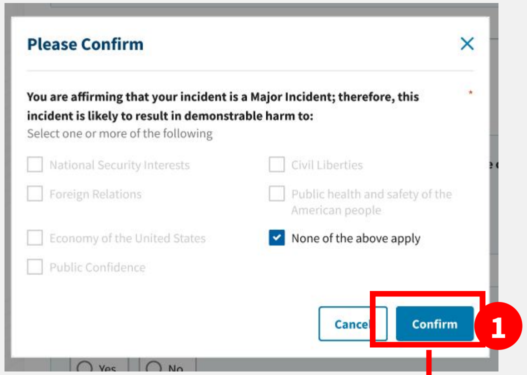
- □ unauthorized modification
- □ unauthorized deletion
- □ unauthorized exfiltration
- □ unauthorized access
- □ loss
- □ theft
- □ inadvertent disclosure

□ **None of the above apply**

Condition 2 Flow

1. If user selects **"None of above apply"** and clicks confirm, follow up questions will then determine if the incident is indeed a major incident.
2. If user selects **any of the PII options** (not just otherwise compromised) the option of **"and is likely to result in demonstrable harm"** will appear.
3. The user then **selects one or more** options from the **"demonstrable harm"** list. This will confirm the incident is a major incident.

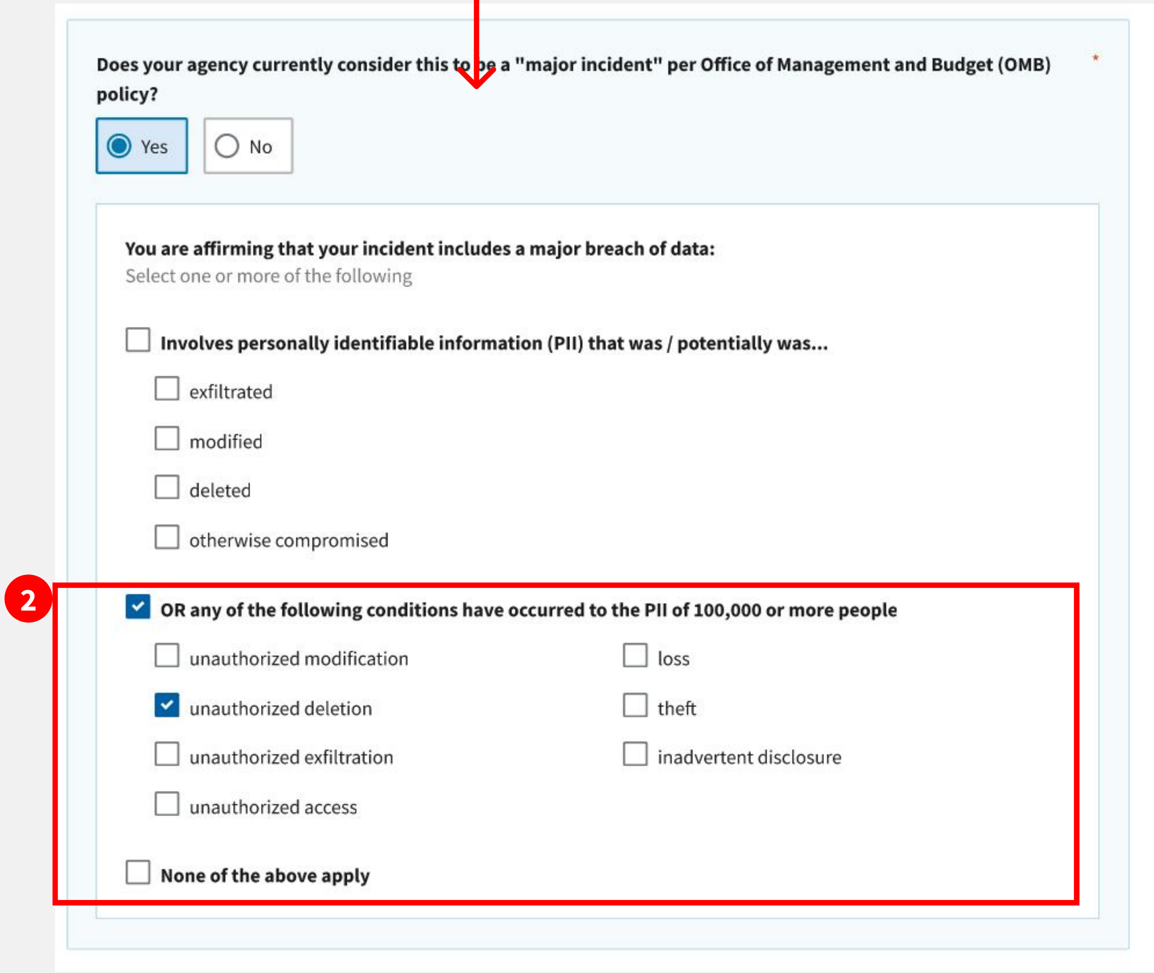
Major Incident - Condition 3



You are affirming that your incident is a Major Incident; therefore, this incident is likely to result in demonstrable harm to: *

Select one or more of the following

- □ National Security Interests
- □ Foreign Relations
- □ Economy of the United States
- □ Public Confidence
- □ Civil Liberties
- □ Public health and safety of the American people
- ☑ None of the above apply



Does your agency currently consider this to be a "major incident" per Office of Management and Budget (OMB) policy? *

● Yes ○ No

You are affirming that your incident includes a major breach of data:

Select one or more of the following

□ Involves personally identifiable information (PII) that was / potentially was...

- □ exfiltrated
- □ modified
- □ deleted
- □ otherwise compromised

☑ OR any of the following conditions have occurred to the PII of 100,000 or more people

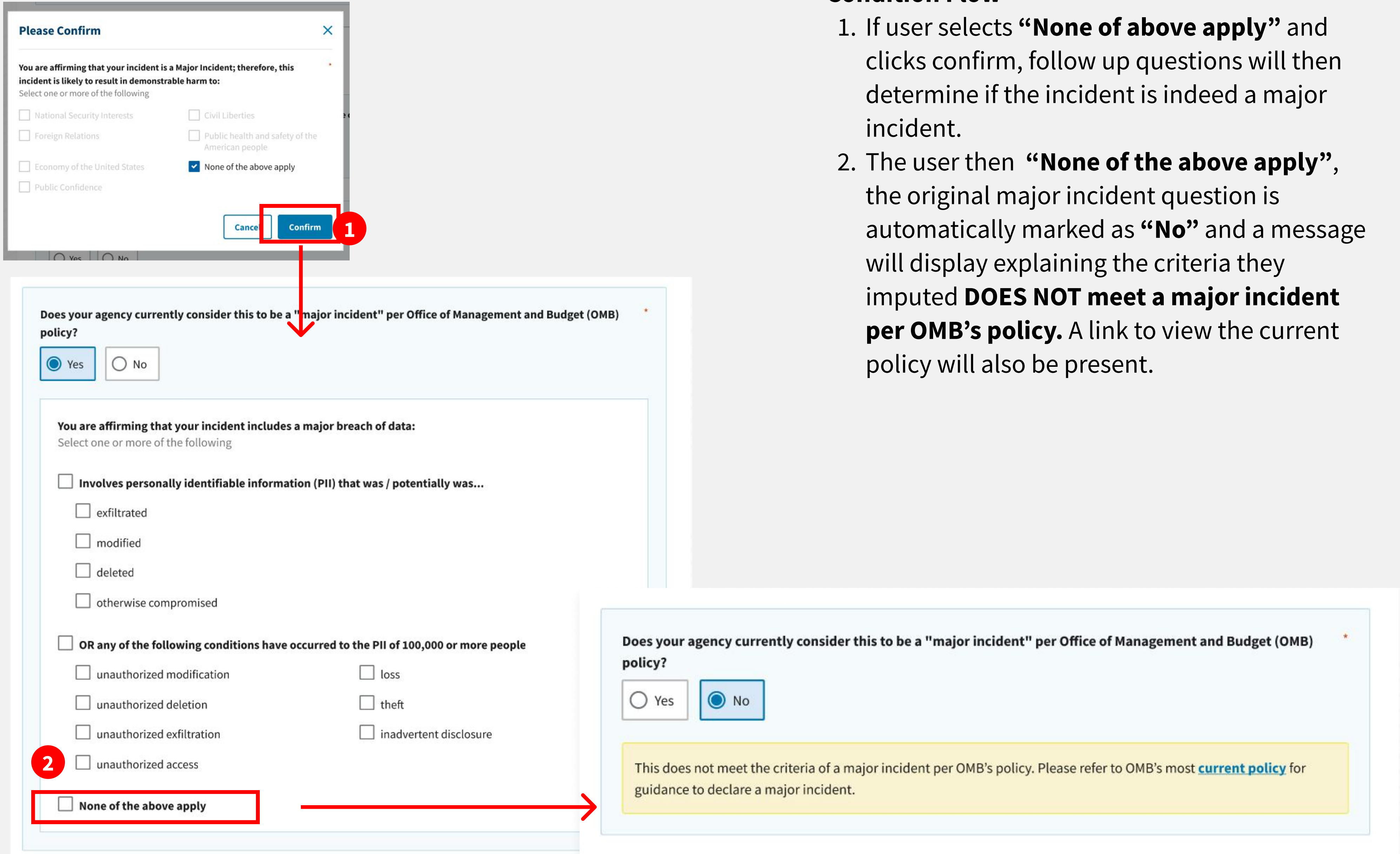
- □ unauthorized modification
- ☑ unauthorized deletion
- □ unauthorized exfiltration
- □ unauthorized access
- □ loss
- □ theft
- □ inadvertent disclosure

□ None of the above apply

Condition 3 Flow

1. If user selects **“None of above apply”** and clicks confirm, follow up questions will then determine if the incident is indeed a major incident.
2. The user then **selects any option** here of an impact against 100,000+ people. This confirms the incident is a major incident.

Major Incident - Not a Major Incident



Please Confirm

You are affirming that your incident is a Major Incident; therefore, this incident is likely to result in demonstrable harm to: *

Select one or more of the following

□ National Security Interests

□ Civil Liberties

□ Foreign Relations

□ Public health and safety of the American people

□ Economy of the United States

☑ None of the above apply

□ Public Confidence

Does your agency currently consider this to be a "major incident" per Office of Management and Budget (OMB) policy? *

● Yes ○ No

You are affirming that your incident includes a major breach of data:

Select one or more of the following

□ Involves personally identifiable information (PII) that was / potentially was...

□ exfiltrated

□ modified

□ deleted

□ otherwise compromised

□ OR any of the following conditions have occurred to the PII of 100,000 or more people

□ unauthorized modification

□ loss

□ unauthorized deletion

□ theft

□ unauthorized exfiltration

□ inadvertent disclosure

□ unauthorized access

□ None of the above apply

Does your agency currently consider this to be a "major incident" per Office of Management and Budget (OMB) policy? *

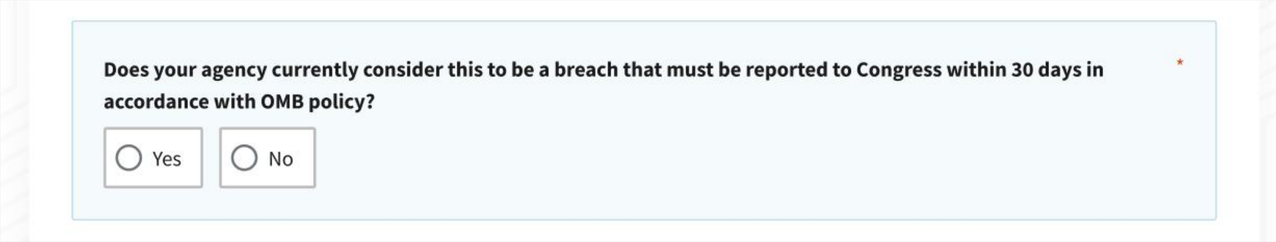
○ Yes ● No

This does not meet the criteria of a major incident per OMB's policy. Please refer to OMB's most **current policy** for guidance to declare a major incident.

Condition Flow

1. If user selects **"None of above apply"** and clicks confirm, follow up questions will then determine if the incident is indeed a major incident.
2. The user then **"None of the above apply"**, the original major incident question is automatically marked as **"No"** and a message will display explaining the criteria they imputed **DOES NOT meet a major incident per OMB's policy.** A link to view the current policy will also be present.

Major Incident



Does your agency currently consider this to be a breach that must be reported to Congress within 30 days in accordance with OMB policy? *

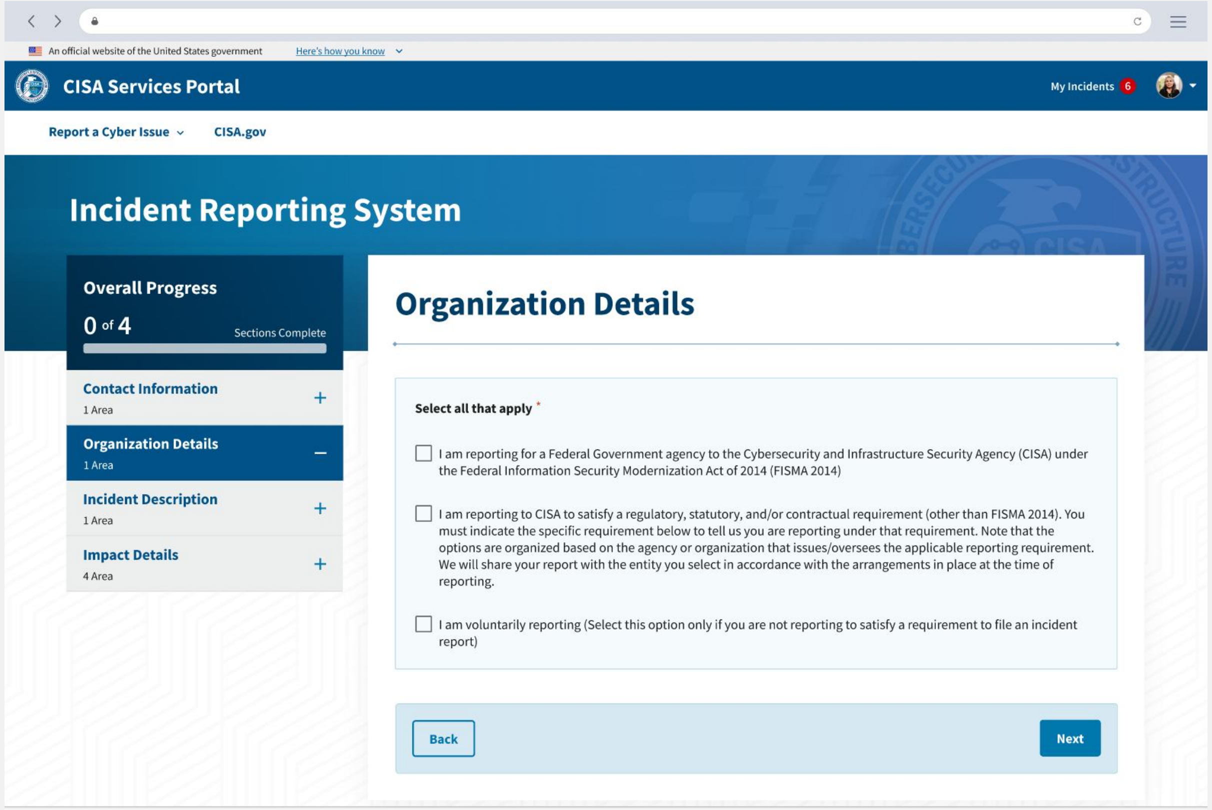
○ Yes ○ No

Flow

Once it has been **determined if the incident is a major incident**, the user will then continue to the next question. This will be a simple YES or NO with no additional follow up questions.

If the incident is not a major incident, the question will not be asked

Organization Details Updates



Organization Details

Select all that apply *

□ I am reporting for a Federal Government agency to the Cybersecurity and Infrastructure Security Agency (CISA) under the Federal Information Security Modernization Act of 2014 (FISMA 2014)

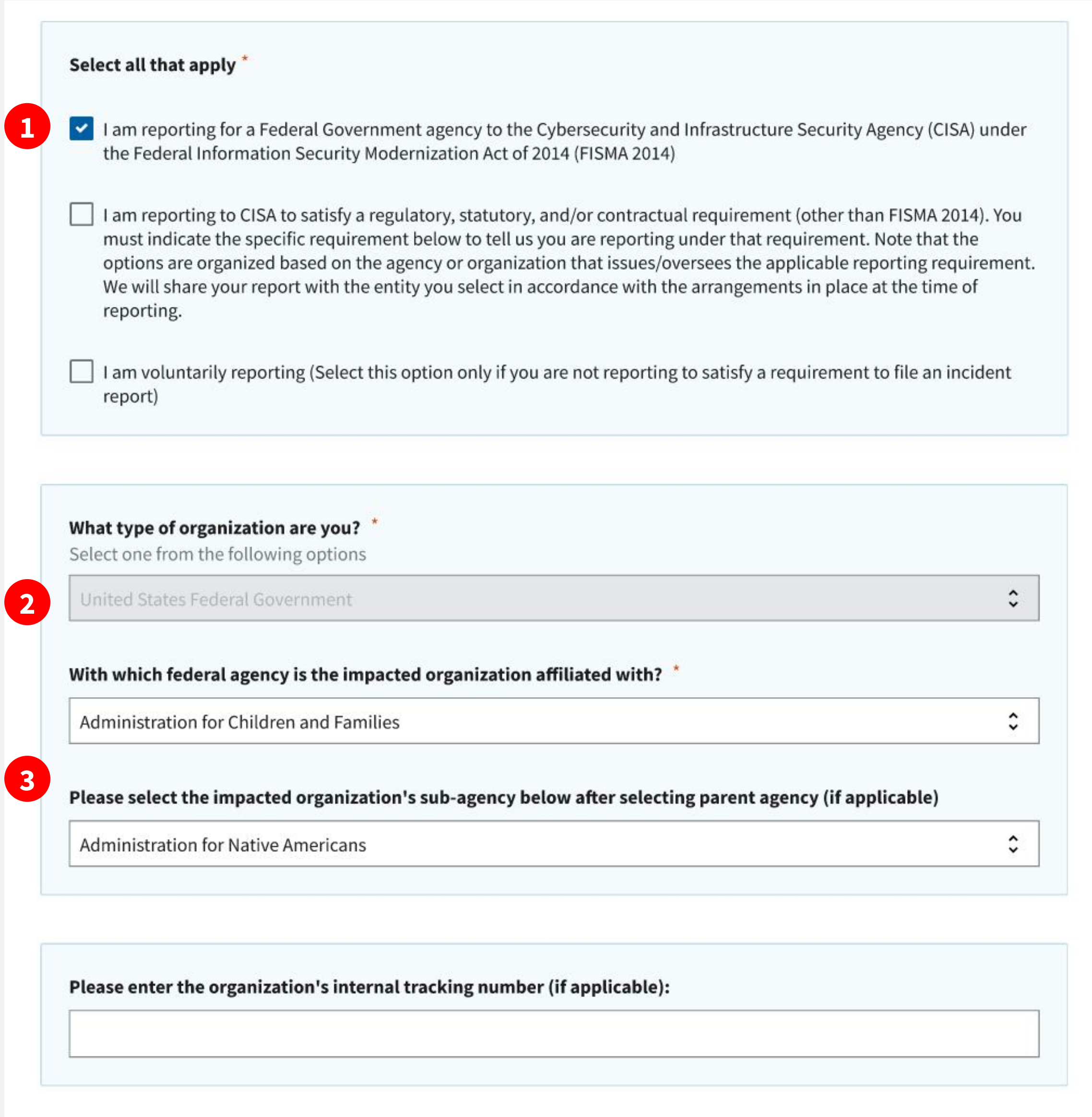
□ I am reporting to CISA to satisfy a regulatory, statutory, and/or contractual requirement (other than FISMA 2014). You must indicate the specific requirement below to tell us you are reporting under that requirement. Note that the options are organized based on the agency or organization that issues/oversees the applicable reporting requirement. We will share your report with the entity you select in accordance with the arrangements in place at the time of reporting.

□ I am voluntarily reporting (Select this option only if you are not reporting to satisfy a requirement to file an incident report)

Notes

- Under Organization Details, before the user selects their organization, they will be asked to answer to select options that apply.
- Their selection here, will determine the follow up questions that will appear.

Organization Details Updates



Select all that apply *

1 ☑ I am reporting for a Federal Government agency to the Cybersecurity and Infrastructure Security Agency (CISA) under the Federal Information Security Modernization Act of 2014 (FISMA 2014)

□ I am reporting to CISA to satisfy a regulatory, statutory, and/or contractual requirement (other than FISMA 2014). You must indicate the specific requirement below to tell us you are reporting under that requirement. Note that the options are organized based on the agency or organization that issues/oversees the applicable reporting requirement. We will share your report with the entity you select in accordance with the arrangements in place at the time of reporting.

□ I am voluntarily reporting (Select this option only if you are not reporting to satisfy a requirement to file an incident report)

What type of organization are you? *

Select one from the following options

2 United States Federal Government

With which federal agency is the impacted organization affiliated with? *

Administration for Children and Families

3 Please select the impacted organization's sub-agency below after selecting parent agency (if applicable)

Administration for Native Americans

Please enter the organization's internal tracking number (if applicable):

User selects:

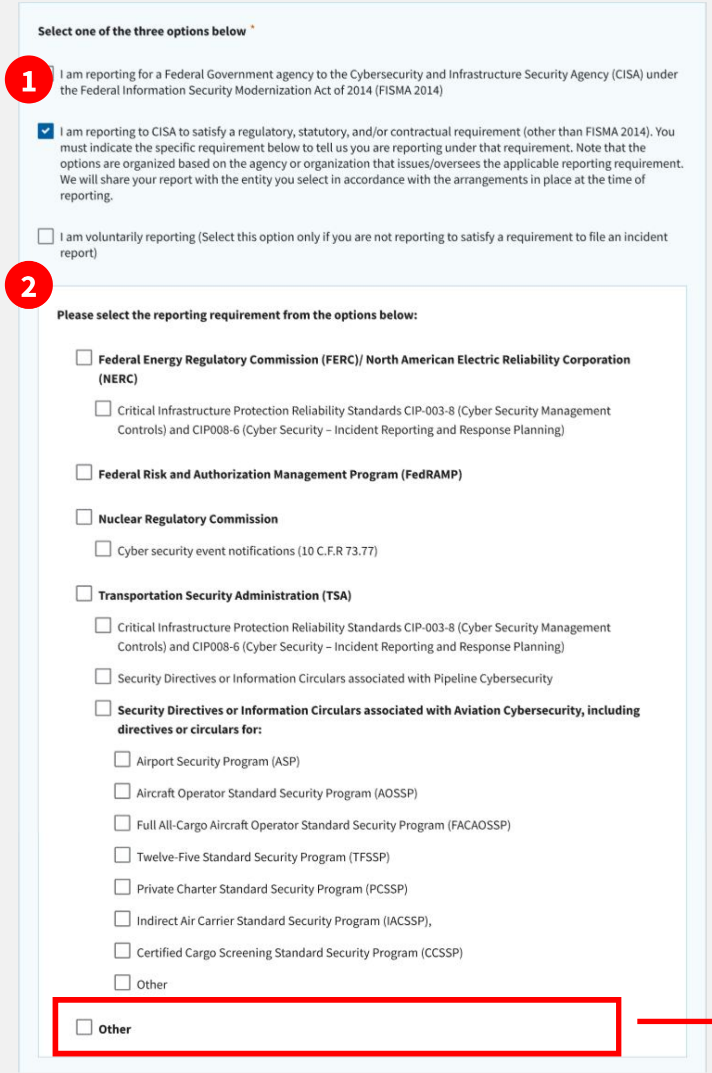
“I am reporting for a Federal Government...”

1. If the user selects this option, the follow up organization details questions will appear.

2. The “What type of organization are you” question will be pre-filled to “**United States Federal Government**”

3. The user will then select the appropriate federal agency and sub agency

Organization Details Updates



Select one of the three options below *

□ I am reporting for a Federal Government agency to the Cybersecurity and Infrastructure Security Agency (CISA) under the Federal Information Security Modernization Act of 2014 (FISMA 2014)

☑ I am reporting to CISA to satisfy a regulatory, statutory, and/or contractual requirement (other than FISMA 2014). You must indicate the specific requirement below to tell us you are reporting under that requirement. Note that the options are organized based on the agency or organization that issues/oversees the applicable reporting requirement. We will share your report with the entity you select in accordance with the arrangements in place at the time of reporting.

□ I am voluntarily reporting (Select this option only if you are not reporting to satisfy a requirement to file an incident report)

Please select the reporting requirement from the options below:

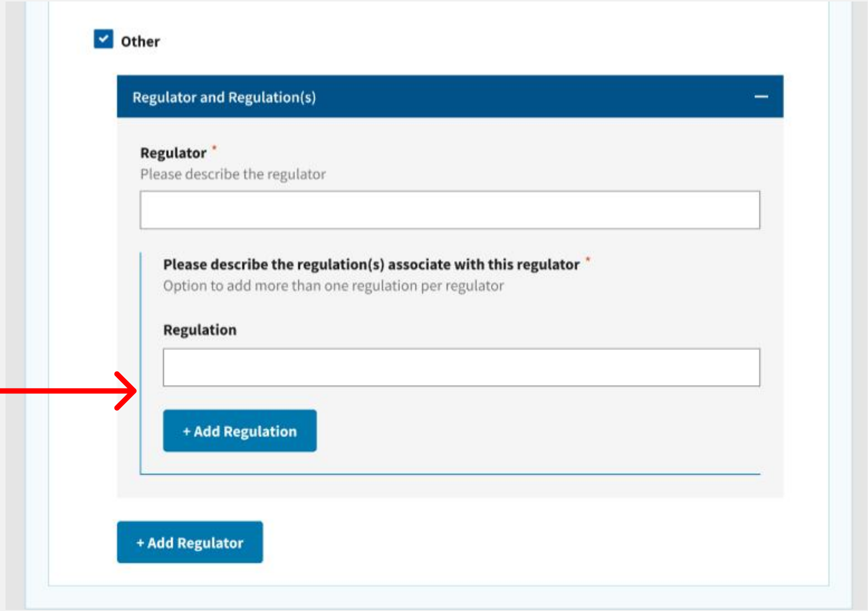
- □ **Federal Energy Regulatory Commission (FERC)/ North American Electric Reliability Corporation (NERC)**
  - □ Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security Management Controls) and CIP008-6 (Cyber Security – Incident Reporting and Response Planning)
- □ **Federal Risk and Authorization Management Program (FedRAMP)**
- □ **Nuclear Regulatory Commission**
  - □ Cyber security event notifications (10 C.F.R 73.77)
- □ **Transportation Security Administration (TSA)**
  - □ Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security Management Controls) and CIP008-6 (Cyber Security – Incident Reporting and Response Planning)
  - □ Security Directives or Information Circulars associated with Pipeline Cybersecurity
  - □ **Security Directives or Information Circulars associated with Aviation Cybersecurity, including directives or circulars for:**
    - □ Airport Security Program (ASP)
    - □ Aircraft Operator Standard Security Program (AOSSP)
    - □ Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP)
    - □ Twelve-Five Standard Security Program (TFSSP)
    - □ Private Charter Standard Security Program (PCSSP)
    - □ Indirect Air Carrier Standard Security Program (IACSSP),
    - □ Certified Cargo Screening Standard Security Program (CCSSP)
    - □ Other
- □ **Other**

User selects:

“I am reporting to CISA to satisfy a regulatory…”

1. If the user selects this option, the user will then be presented with a series of check boxes
2. Here the user will be ask to select their applicable reporting requirements.

Note: If the user selects **“other”**, they will be asked to enter a **“Regulator”** and any related **“Regulations”.** The user will have to option to additional related regulations. The user will also have the option to add additional regulators with it’s own set of regulations.



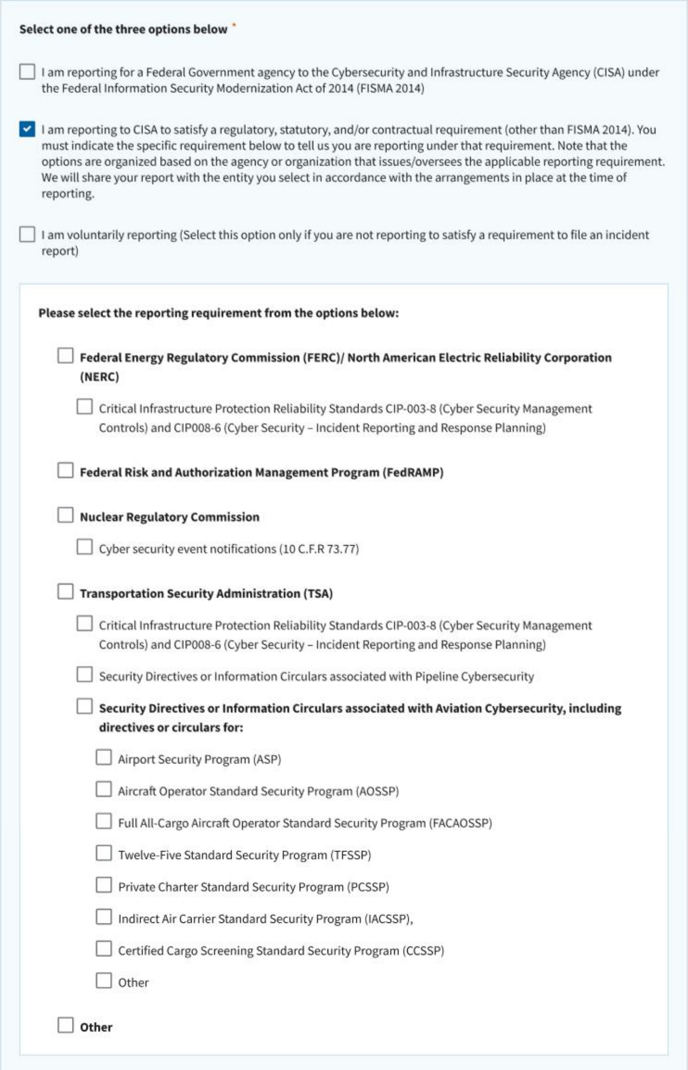
☑ Other

Regulator *
Please describe the regulator

Please describe the regulation(s) associate with this regulator *
Option to add more than one regulation per regulator

Regulation

Organization Details Updates



Select one of the three options below *

☐ I am reporting for a Federal Government agency to the Cybersecurity and Infrastructure Security Agency (CISA) under the Federal Information Security Modernization Act of 2014 (FISMA 2014)

☑ I am reporting to CISA to satisfy a regulatory, statutory, and/or contractual requirement (other than FISMA 2014). You must indicate the specific requirement below to tell us you are reporting under that requirement. Note that the options are organized based on the agency or organization that issues/oversees the applicable reporting requirement. We will share your report with the entity you select in accordance with the arrangements in place at the time of reporting.

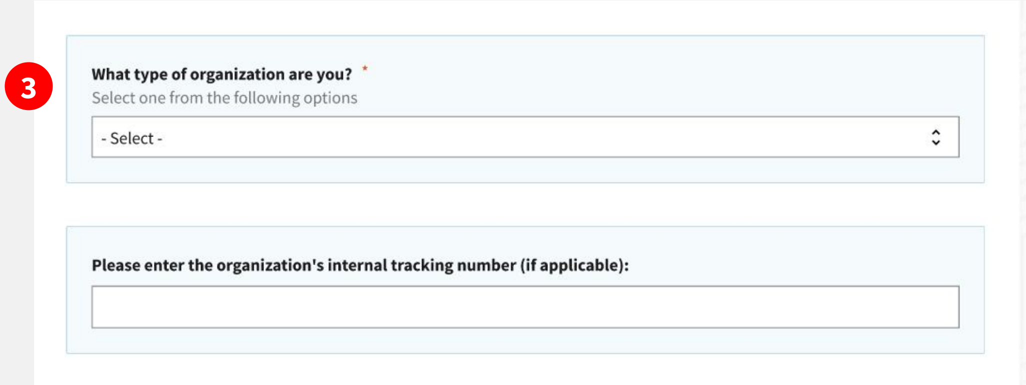
☐ I am voluntarily reporting (Select this option only if you are not reporting to satisfy a requirement to file an incident report)

Please select the reporting requirement from the options below:

- ☐ **Federal Energy Regulatory Commission (FERC)/ North American Electric Reliability Corporation (NERC)**
  - ☐ Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security Management Controls) and CIP008-6 (Cyber Security – Incident Reporting and Response Planning)
- ☐ **Federal Risk and Authorization Management Program (FedRAMP)**
- ☐ **Nuclear Regulatory Commission**
  - ☐ Cyber security event notifications (10 C.F.R 73.77)
- ☐ **Transportation Security Administration (TSA)**
  - ☐ Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security Management Controls) and CIP008-6 (Cyber Security – Incident Reporting and Response Planning)
  - ☐ Security Directives or Information Circulars associated with Pipeline Cybersecurity
  - ☐ **Security Directives or Information Circulars associated with Aviation Cybersecurity, including directives or circulars for:**
    - ☐ Airport Security Program (ASP)
    - ☐ Aircraft Operator Standard Security Program (AOSSP)
    - ☐ Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP)
    - ☐ Twelve-Five Standard Security Program (TFSSP)
    - ☐ Private Charter Standard Security Program (PCSSP)
    - ☐ Indirect Air Carrier Standard Security Program (IACSSP),
    - ☐ Certified Cargo Screening Standard Security Program (CCSSP)
    - ☐ Other
- ☐ **Other**

3. Once completed, the user will then select the type of organization from a drop-down. Depending on the the organization selected, follow up questions regarding that particular organization will appear.

   Lastly, the user can enter the org tracking number if applicable.



3

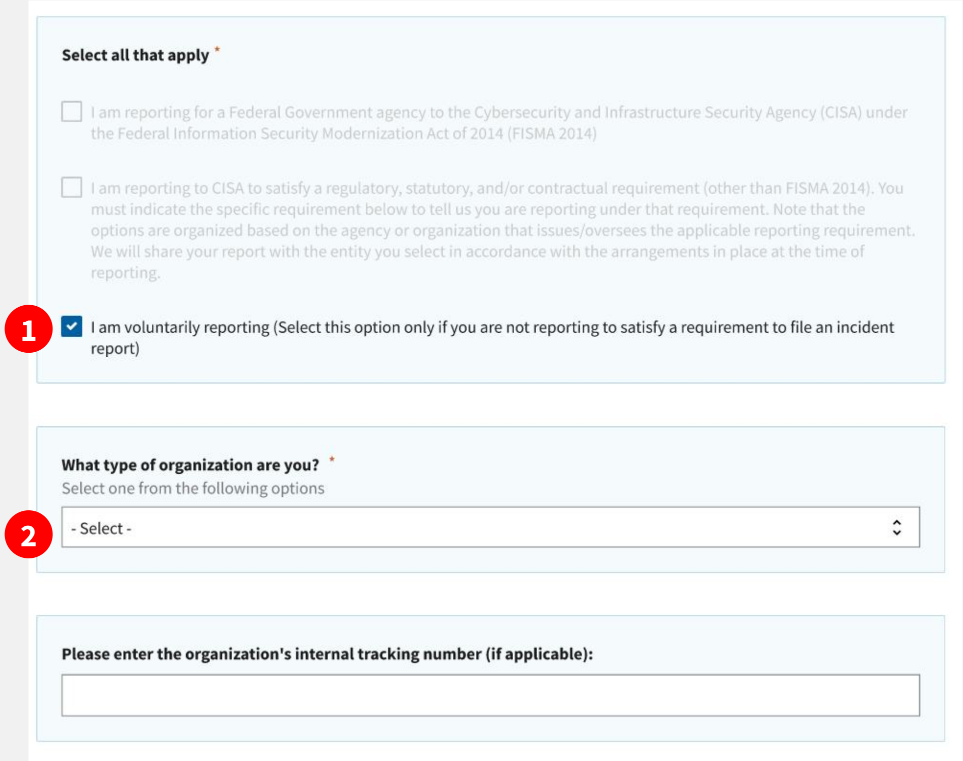
What type of organization are you? *

Select one from the following options

- Select -

Please enter the organization's internal tracking number (if applicable):

Organization Details Updates



Select all that apply *

□ I am reporting for a Federal Government agency to the Cybersecurity and Infrastructure Security Agency (CISA) under the Federal Information Security Modernization Act of 2014 (FISMA 2014)

□ I am reporting to CISA to satisfy a regulatory, statutory, and/or contractual requirement (other than FISMA 2014). You must indicate the specific requirement below to tell us you are reporting under that requirement. Note that the options are organized based on the agency or organization that issues/oversees the applicable reporting requirement. We will share your report with the entity you select in accordance with the arrangements in place at the time of reporting.

1 ☑ I am voluntarily reporting (Select this option only if you are not reporting to satisfy a requirement to file an incident report)

What type of organization are you? *

Select one from the following options

2 - Select -

Please enter the organization's internal tracking number (if applicable):

User selects:

"I am voluntarily reporting..."

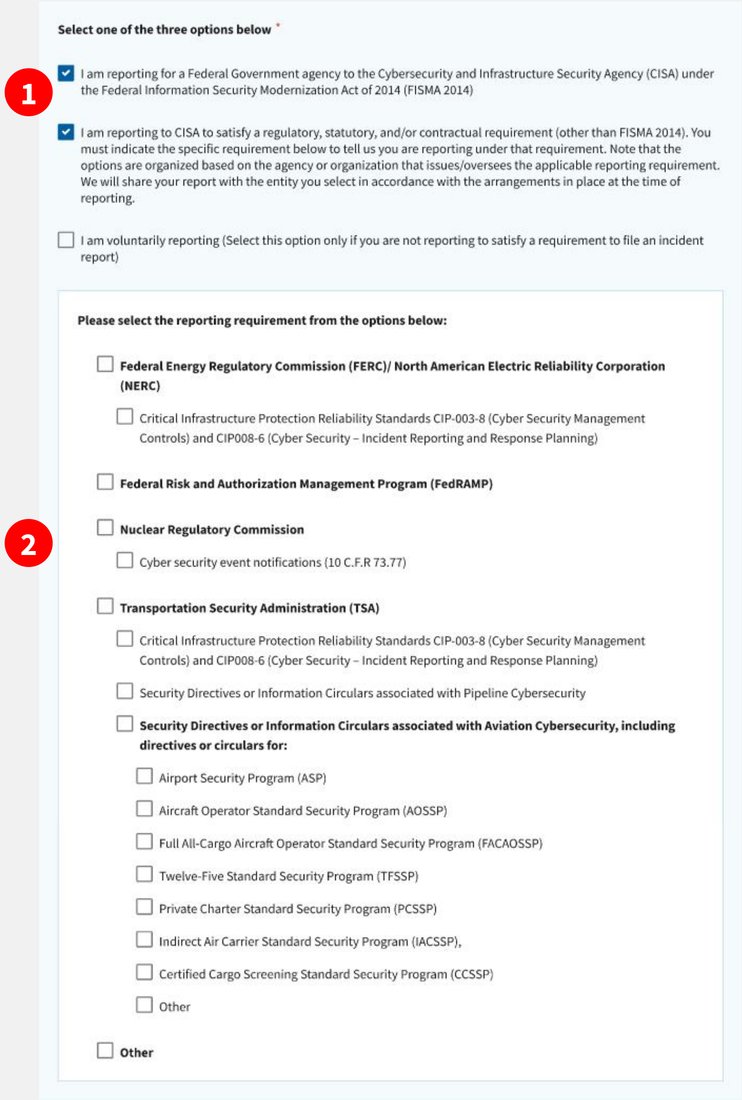
1. If the user selects this option, the first two options will be disabled as they are not applicable with this selection.

2. Once completed, the user will then select the type of organization from a drop-down. Depending on the the organization selected, follow up questions regarding that particular organization will appear.

   Lastly, the user can enter the org tracking number if applicable.

   NOTE: The user can uncheck this selection to enable the first two options

Organization Details Updates



Select one of the three options below *

☑ I am reporting for a Federal Government agency to the Cybersecurity and Infrastructure Security Agency (CISA) under the Federal Information Security Modernization Act of 2014 (FISMA 2014)

☑ I am reporting to CISA to satisfy a regulatory, statutory, and/or contractual requirement (other than FISMA 2014). You must indicate the specific requirement below to tell us you are reporting under that requirement. Note that the options are organized based on the agency or organization that issues/oversees the applicable reporting requirement. We will share your report with the entity you select in accordance with the arrangements in place at the time of reporting.

☐ I am voluntarily reporting (Select this option only if you are not reporting to satisfy a requirement to file an incident report)

Please select the reporting requirement from the options below:

- ☐ **Federal Energy Regulatory Commission (FERC)/ North American Electric Reliability Corporation (NERC)**
  - ☐ Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security Management Controls) and CIP008-6 (Cyber Security – Incident Reporting and Response Planning)
- ☐ **Federal Risk and Authorization Management Program (FedRAMP)**
- ☐ **Nuclear Regulatory Commission**
  - ☐ Cyber security event notifications (10 C.F.R 73.77)
- ☐ **Transportation Security Administration (TSA)**
  - ☐ Critical Infrastructure Protection Reliability Standards CIP-003-8 (Cyber Security Management Controls) and CIP008-6 (Cyber Security – Incident Reporting and Response Planning)
  - ☐ Security Directives or Information Circulars associated with Pipeline Cybersecurity
  - ☐ **Security Directives or Information Circulars associated with Aviation Cybersecurity, including directives or circulars for:**
    - ☐ Airport Security Program (ASP)
    - ☐ Aircraft Operator Standard Security Program (AOSSP)
    - ☐ Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP)
    - ☐ Twelve-Five Standard Security Program (TFSSP)
    - ☐ Private Charter Standard Security Program (PCSSP)
    - ☐ Indirect Air Carrier Standard Security Program (IACSSP),
    - ☐ Certified Cargo Screening Standard Security Program (CCSSP)
    - ☐ Other
- ☐ **Other**

User selects:

"I am reporting for a Federal Government..."

AND

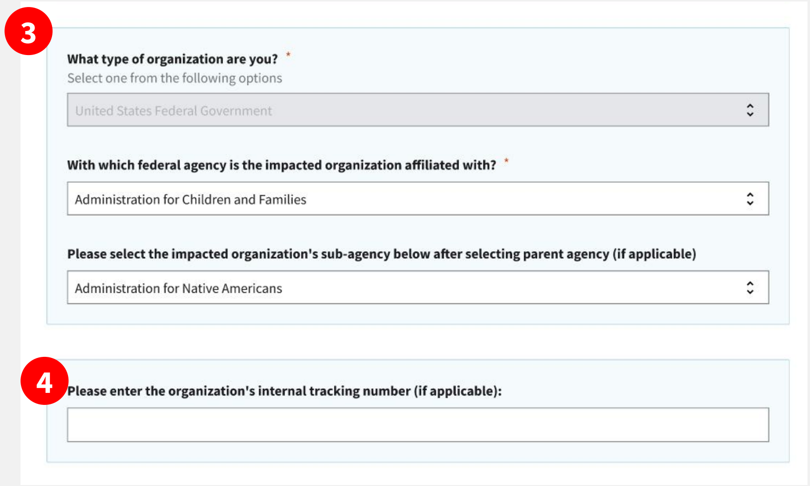
"I am reporting to CISA to satisfy a regulatory..."

1. The user selects BOTH these options together

2. Here the user will be ask to select their applicable reporting requirements.

3. The "What type of organization are you" question will be pre-filled to "**United States Federal Government**"

4. The user will then select the appropriate federal agency and sub agency



What type of organization are you? *
Select one from the following options

United States Federal Government

With which federal agency is the impacted organization affiliated with? *

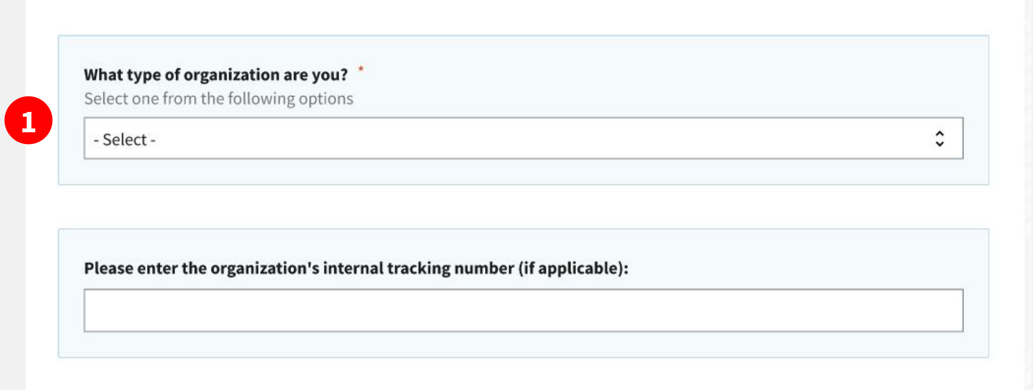
Administration for Children and Families

Please select the impacted organization's sub-agency below after selecting parent agency (if applicable)

Administration for Native Americans

Please enter the organization's internal tracking number (if applicable):

Critical Infrastructure Updates



What type of organization are you? *
Select one from the following options

- Select -

Please enter the organization's internal tracking number (if applicable):

Notes

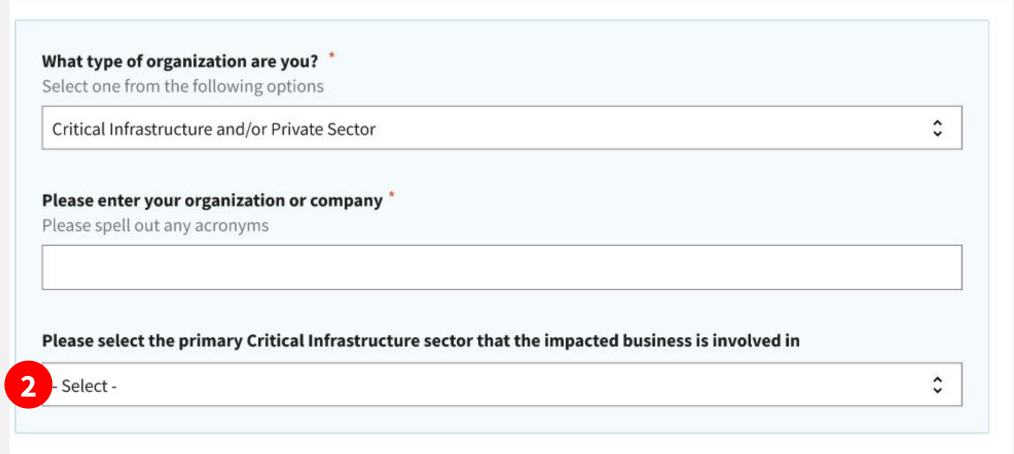
- This is located under the **Organization Details** section
- This update asks an additional question when the user selects **“Critical Infrastructure/ Private industry”** as their organization

Flow

1. The user selects **“Critical Infrastructure/ Private industry”** as their organization

2. User selects the associated Sector

3. A new drop-down will appear, asking the user to select their sector’s associated sub-sector.



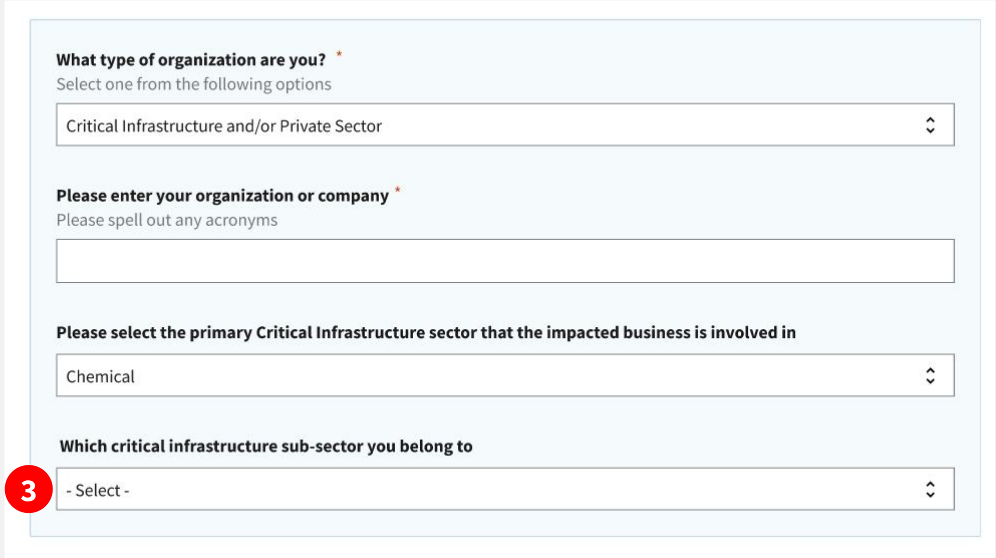
What type of organization are you? *
Select one from the following options

Critical Infrastructure and/or Private Sector

Please enter your organization or company *
Please spell out any acronyms

Please select the primary Critical Infrastructure sector that the impacted business is involved in

- Select -



What type of organization are you? *
Select one from the following options

Critical Infrastructure and/or Private Sector

Please enter your organization or company *
Please spell out any acronyms

Please select the primary Critical Infrastructure sector that the impacted business is involved in

Chemical

Which critical infrastructure sub-sector you belong to

- Select -