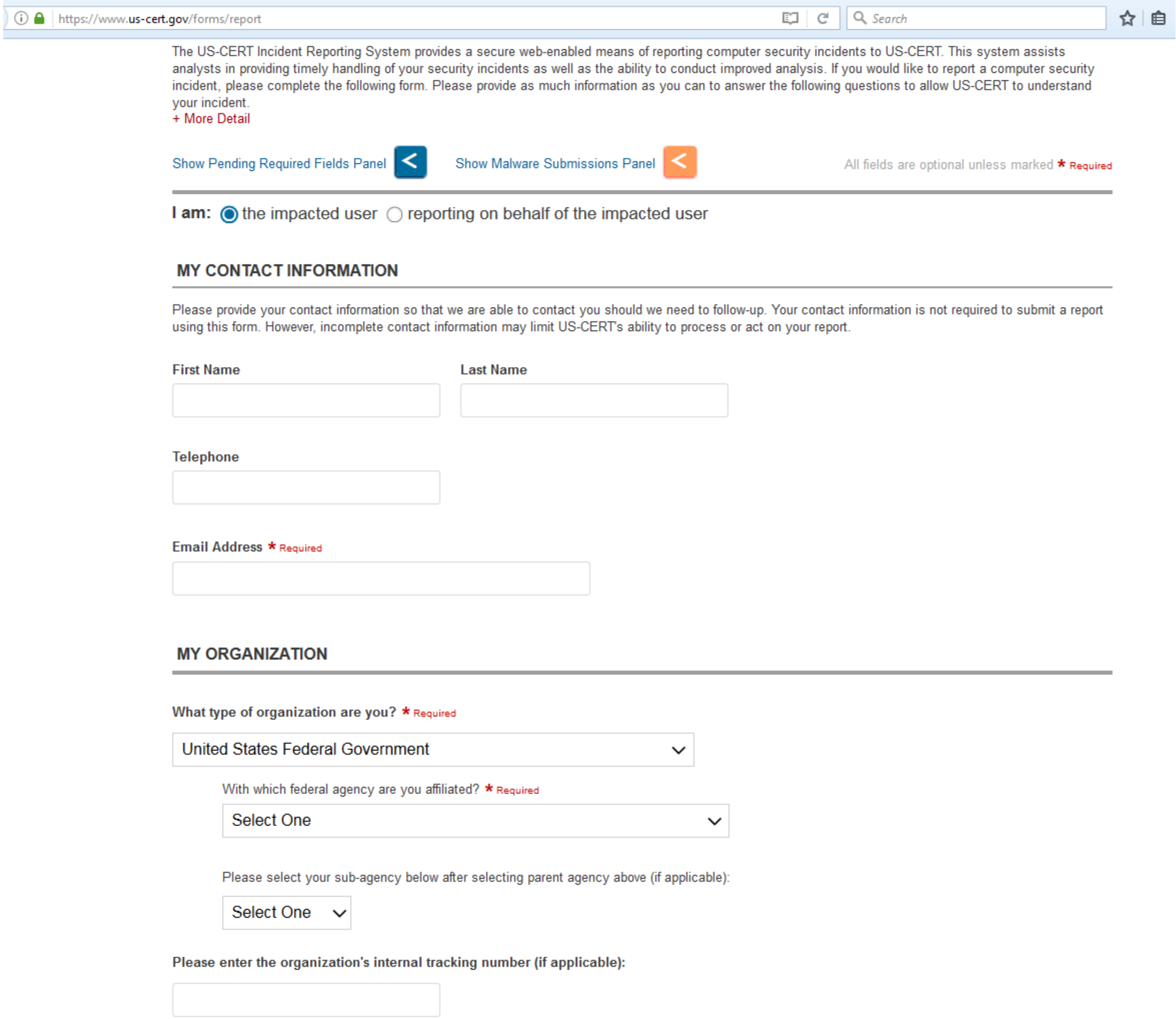
OMB Control Number: 1670-NEW
OMB Expiration Date: MM/DD/YYYY

Paperwork Reduction Act

The public reporting burden to complete this information collection is estimated at 3 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the collected information. The collection of information is 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/NPPD/CS&C/NCCIC/US-CERT, 245 Murray Lane, SW, Mail Stop 0640, Arlington, VA 20598-0640 ATTN: PRA [*OMB Control No. 1670-NEW*].

Incident Reporting Form

https://www.us-cert.gov/forms/report



The US-CERT Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to US-CERT. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis. If you would like to report a computer security incident, please complete the following form. Please provide as much information as you can to answer the following questions to allow US-CERT to understand your incident.

+ More Detail

Show Pending Required Fields Panel <   Show Malware Submissions Panel <   All fields are optional unless marked * Required

I am: ● the impacted user ○ reporting on behalf of the impacted user

MY CONTACT INFORMATION

Please provide your contact information so that we are able to contact you should we need to follow-up. Your contact information is not required to submit a report using this form. However, incomplete contact information may limit US-CERT's ability to process or act on your report.

First Name ______ **Last Name** ______

Telephone ______

Email Address * Required ______

MY ORGANIZATION

What type of organization are you? * Required

United States Federal Government ⌄

With which federal agency are you affiliated? * Required

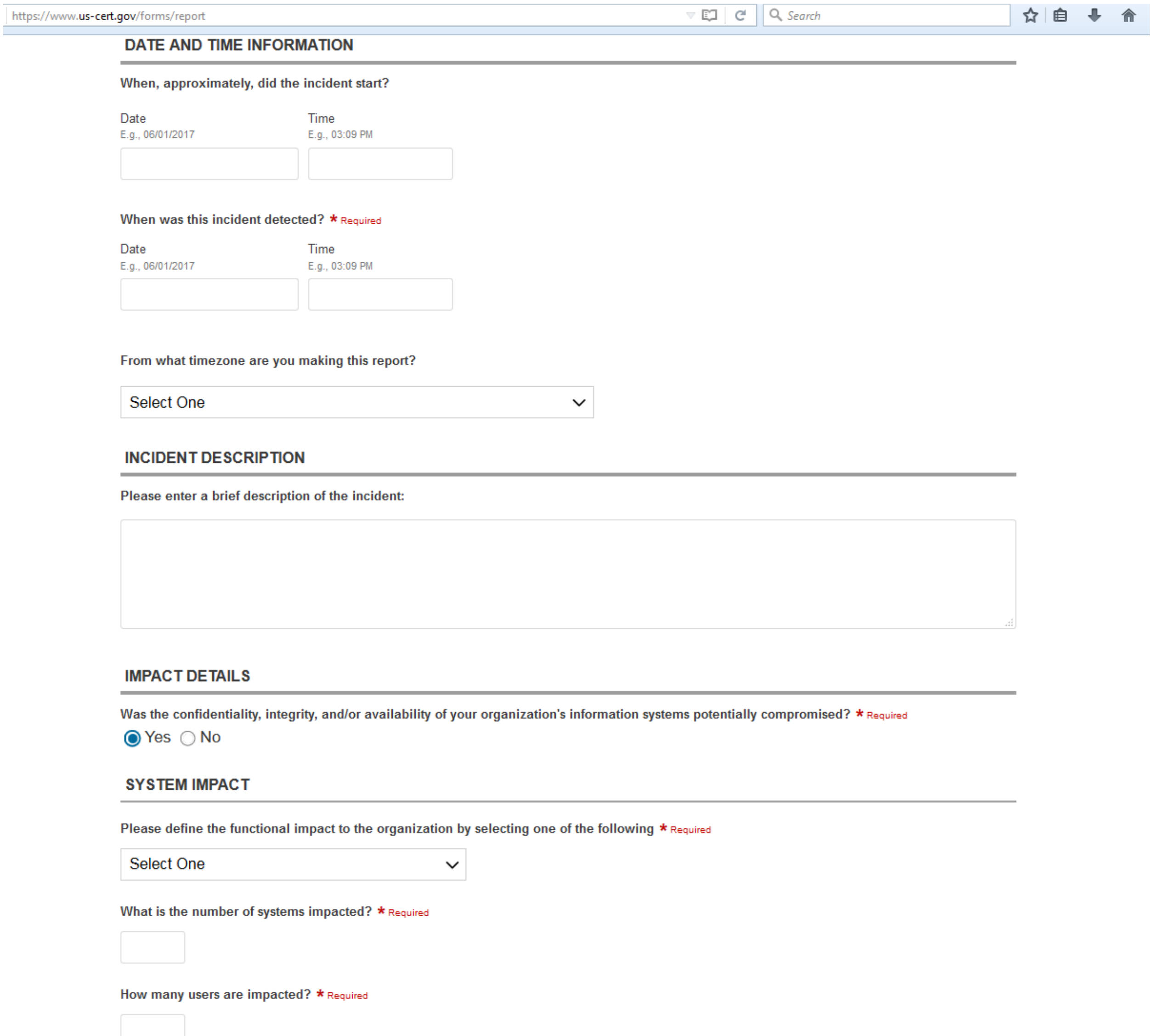
Select One ⌄

Please select your sub-agency below after selecting parent agency above (if applicable):

Select One ⌄

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

______



DATE AND TIME INFORMATION

When, approximately, did the incident start?

Date
E.g., 06/01/2017

Time
E.g., 03:09 PM

When was this incident detected? * Required

Date
E.g., 06/01/2017

Time
E.g., 03:09 PM

From what timezone are you making this report?

Select One

INCIDENT DESCRIPTION

Please enter a brief description of the incident:

IMPACT DETAILS

Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised? * Required

● Yes ○ No

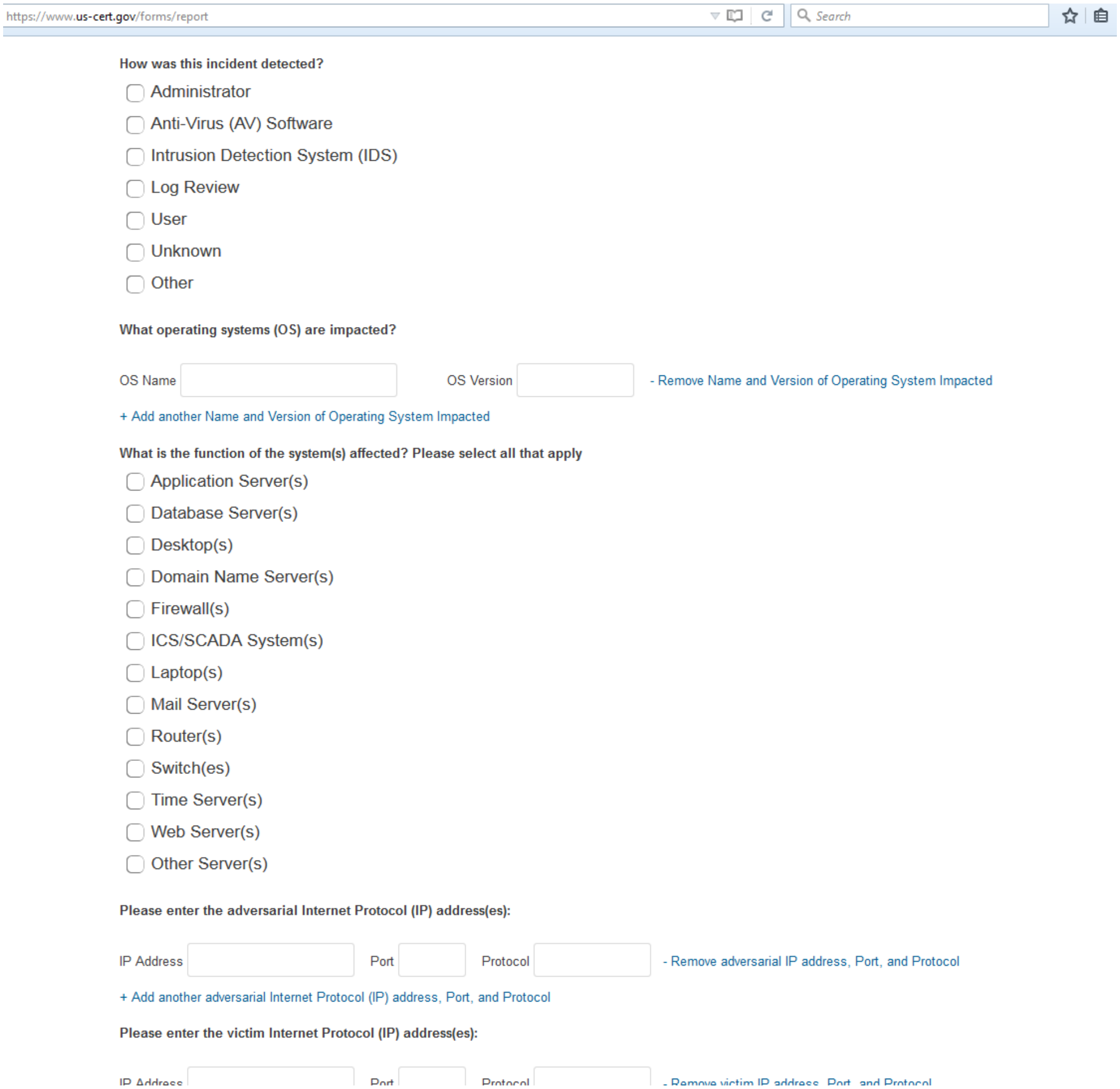
SYSTEM IMPACT

Please define the functional impact to the organization by selecting one of the following * Required

Select One

What is the number of systems impacted? * Required

How many users are impacted? * Required



How was this incident detected?

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

What operating systems (OS) are impacted?

OS Name ______ OS Version ______ - Remove Name and Version of Operating System Impacted

+ Add another Name and Version of Operating System Impacted

What is the function of the system(s) affected? Please select all that apply

- □ Application Server(s)
- □ Database Server(s)
- □ Desktop(s)
- □ Domain Name Server(s)
- □ Firewall(s)
- □ ICS/SCADA System(s)
- □ Laptop(s)
- □ Mail Server(s)
- □ Router(s)
- □ Switch(es)
- □ Time Server(s)
- □ Web Server(s)
- □ Other Server(s)

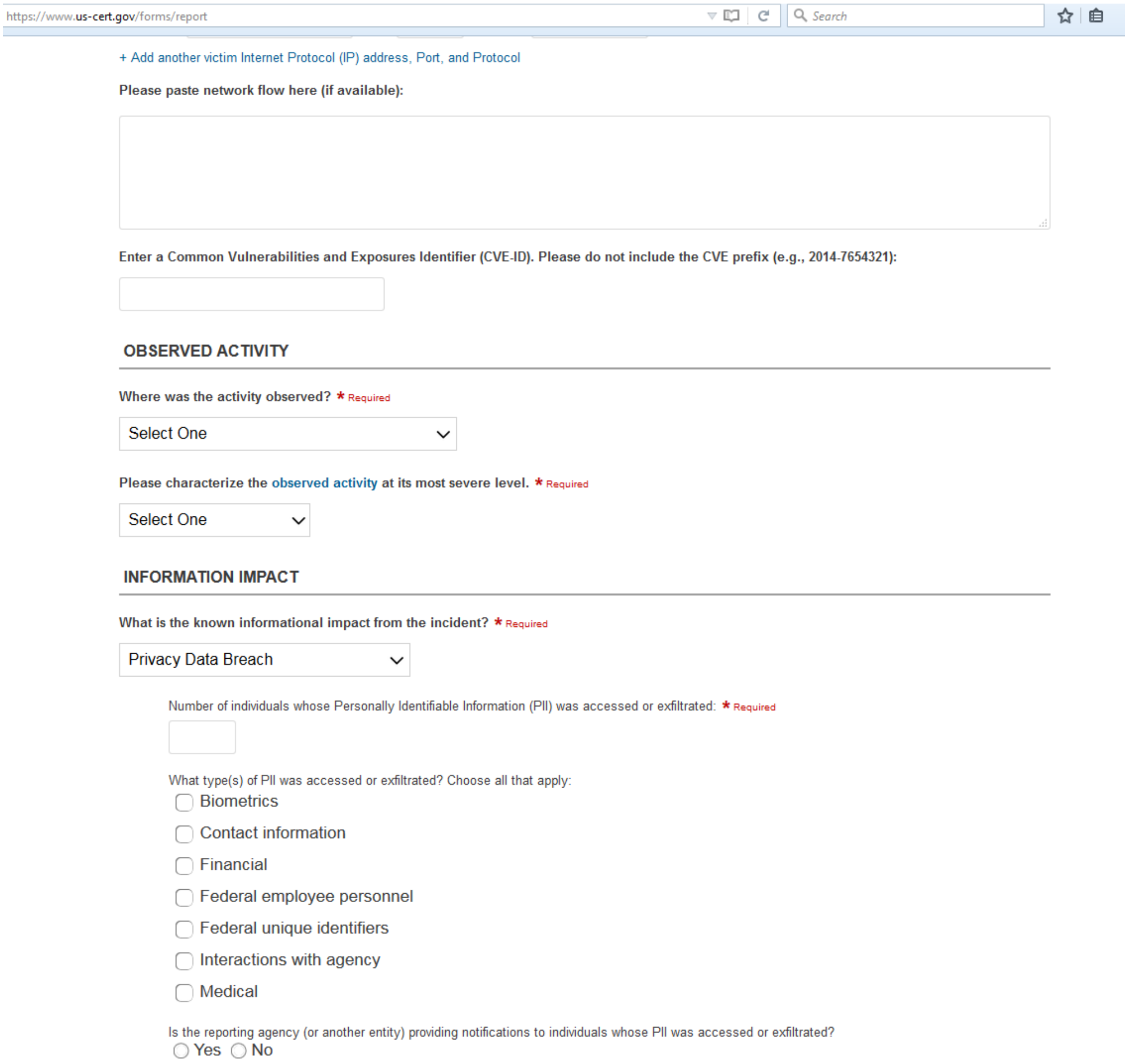
Please enter the adversarial Internet Protocol (IP) address(es):

IP Address ______ Port ______ Protocol ______ - Remove adversarial IP address, Port, and Protocol

+ Add another adversarial Internet Protocol (IP) address, Port, and Protocol

Please enter the victim Internet Protocol (IP) address(es):

IP Address ______ Port ______ Protocol ______ - Remove victim IP address, Port, and Protocol



+ Add another victim Internet Protocol (IP) address, Port, and Protocol

Please paste network flow here (if available):

Enter a Common Vulnerabilities and Exposures Identifier (CVE-ID). Please do not include the CVE prefix (e.g., 2014-7654321):

OBSERVED ACTIVITY

Where was the activity observed? * Required

Select One

Please characterize the observed activity at its most severe level. * Required

Select One

INFORMATION IMPACT

What is the known informational impact from the incident? * Required

Privacy Data Breach

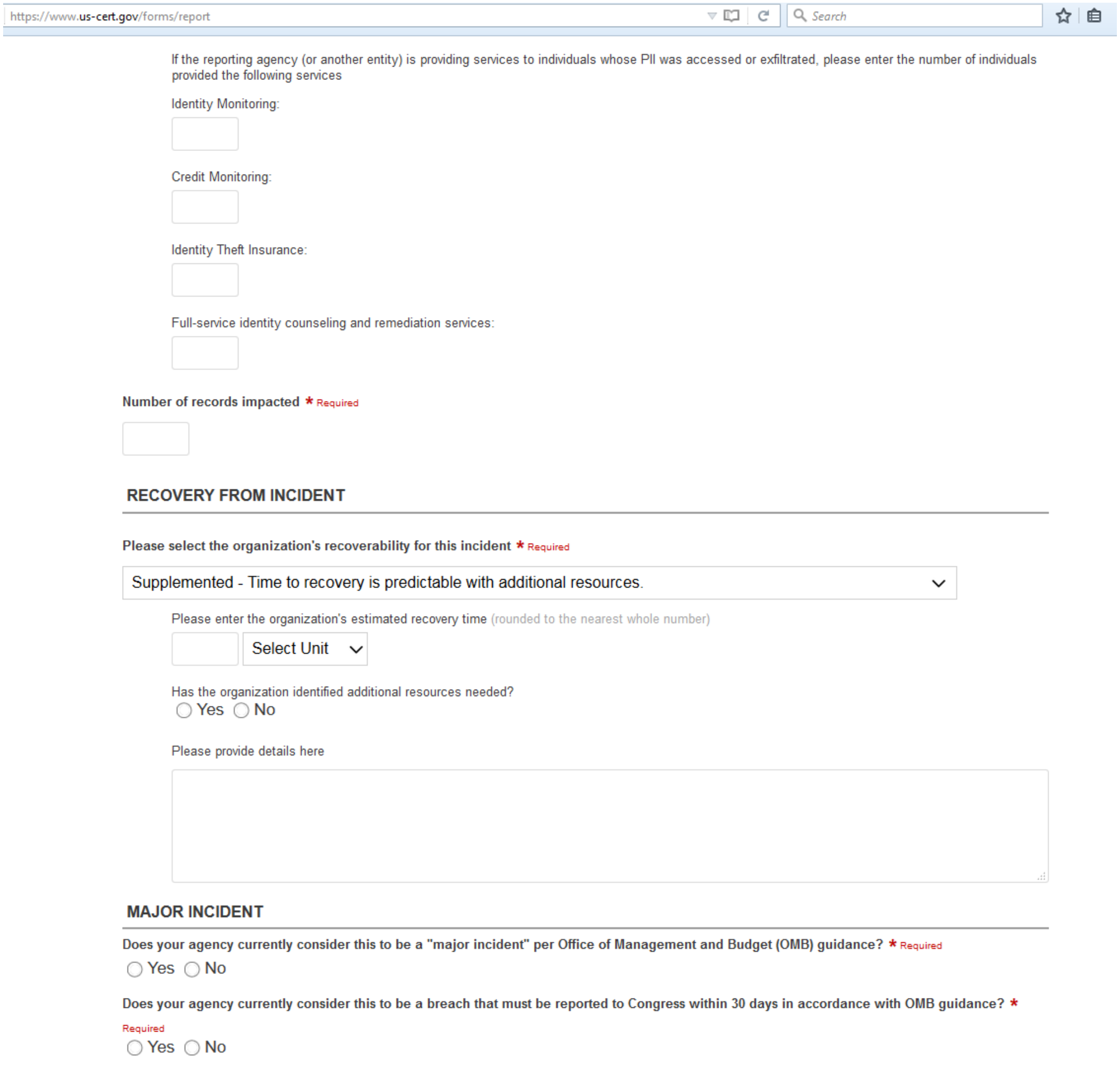
Number of individuals whose Personally Identifiable Information (PII) was accessed or exfiltrated: * Required

What type(s) of PII was accessed or exfiltrated? Choose all that apply:

□ Biometrics
□ Contact information
□ Financial
□ Federal employee personnel
□ Federal unique identifiers
□ Interactions with agency
□ Medical

Is the reporting agency (or another entity) providing notifications to individuals whose PII was accessed or exfiltrated?

○ Yes ○ No



If the reporting agency (or another entity) is providing services to individuals whose PII was accessed or exfiltrated, please enter the number of individuals provided the following services

Identity Monitoring:

Credit Monitoring:

Identity Theft Insurance:

Full-service identity counseling and remediation services:

Number of records impacted * Required

RECOVERY FROM INCIDENT

Please select the organization's recoverability for this incident * Required

Supplemented - Time to recovery is predictable with additional resources.

Please enter the organization's estimated recovery time (rounded to the nearest whole number)

Select Unit

Has the organization identified additional resources needed?
○ Yes ○ No

Please provide details here

MAJOR INCIDENT

Does your agency currently consider this to be a "major incident" per Office of Management and Budget (OMB) guidance? * Required
○ Yes ○ No

Does your agency currently consider this to be a breach that must be reported to Congress within 30 days in accordance with OMB guidance? *
Required
○ Yes ○ No