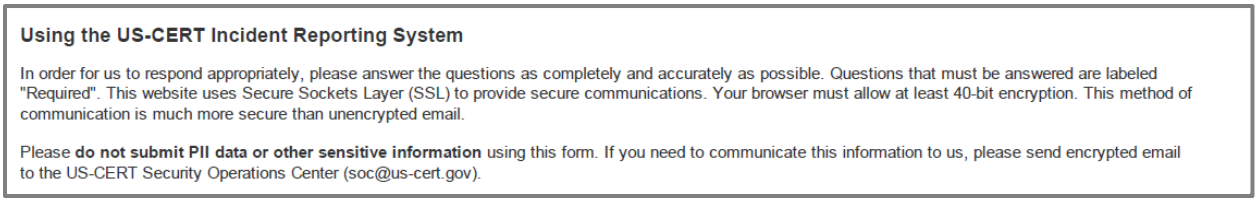
US-CERT Incident Reporting System

UPDATE: As of February 2015, the Department of Homeland Security has issued guidance that only confirmed cybersecurity related breaches must be reported to US-CERT. Non cybersecurity related breaches (i.e., paper) should no longer be reported. However, reporting of suspected cybersecurity incidents is optional if you feel meets the criteria for an incident.

Breach reporting to the United States-Computer Emergency Readiness Team (US-CERT) can be initiated by going to the following link: https://forms.us-cert.gov/report/.

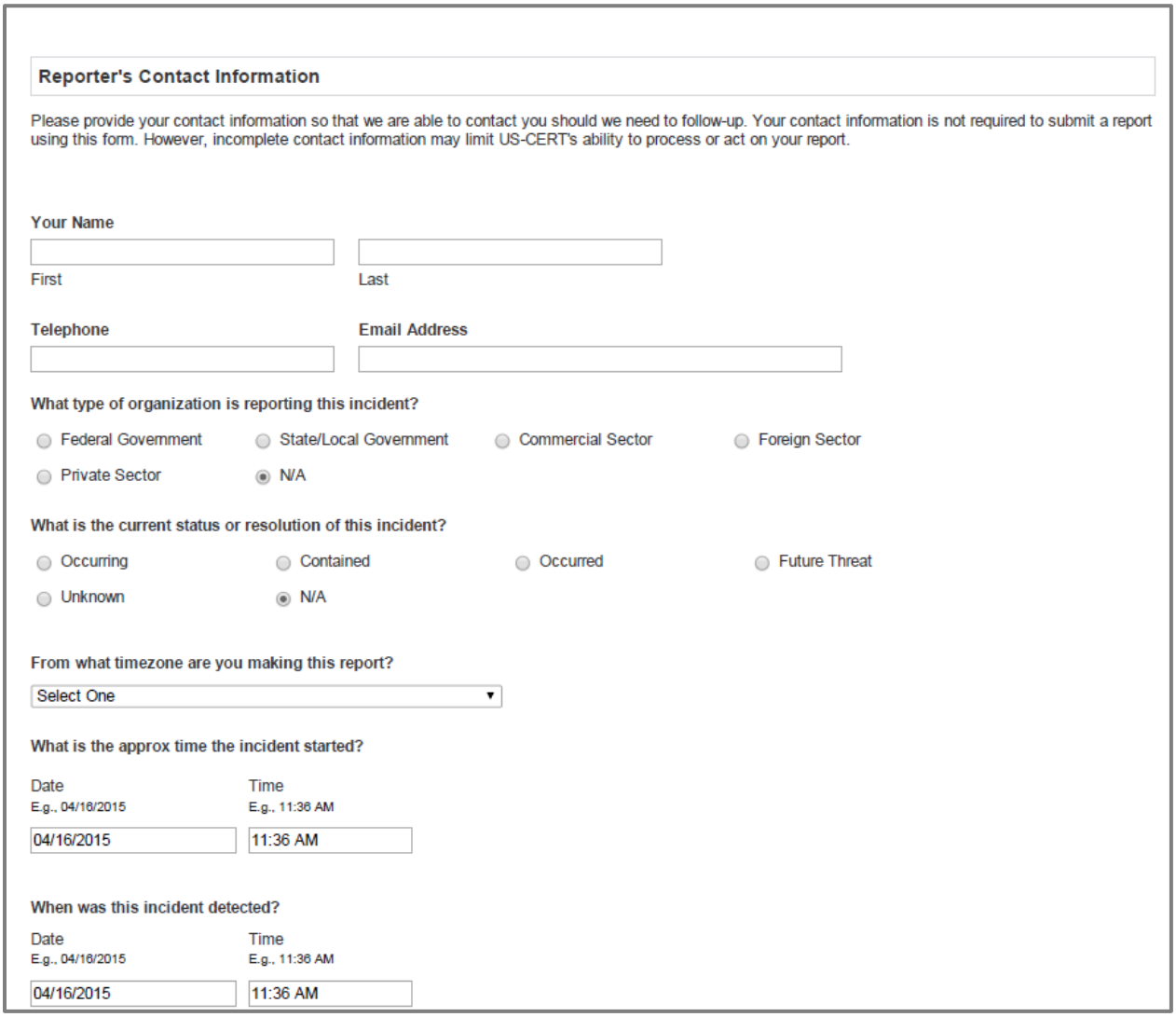
Note: Any updates to the initial report are to be provided via email to soc@us-cert.gov and the assigned US-CERT number must be referenced in the subject line.



By scrolling down on the initial screen, the user is directed to a set of blank fields, which serve to provide the reporter's contact information, a preliminary description of the breach, and the corresponding impact.

Please note that reporting a breach does not assign responsibility or ownership. It is an obligation to promptly inform your Privacy Official in accordance with DoD policy so that requisite steps are taken and properly coordinated.

US-CERT Incident Reporting System



Reporter's 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.

Your Name

First

Last

Telephone

Email Address

What type of organization is reporting this incident?

Federal Government | State/Local Government | Commercial Sector | Foreign Sector | Private Sector | N/A

What is the current status or resolution of this incident?

Occurring | Contained | Occurred | Future Threat | Unknown | N/A

From what timezone are you making this report?

Select One

What is the approx time the incident started?

Date E.g., 04/16/2015: 04/16/2015

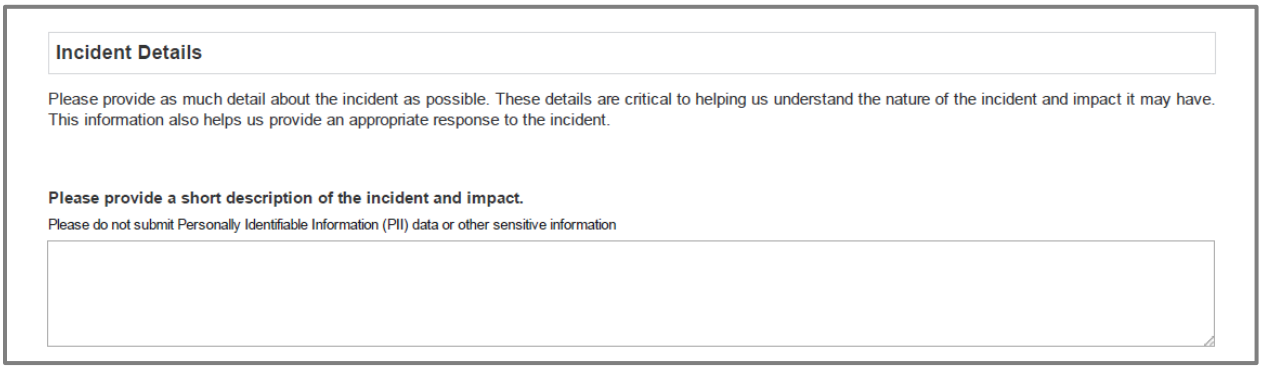
Time E.g., 11:36 AM: 11:36 AM

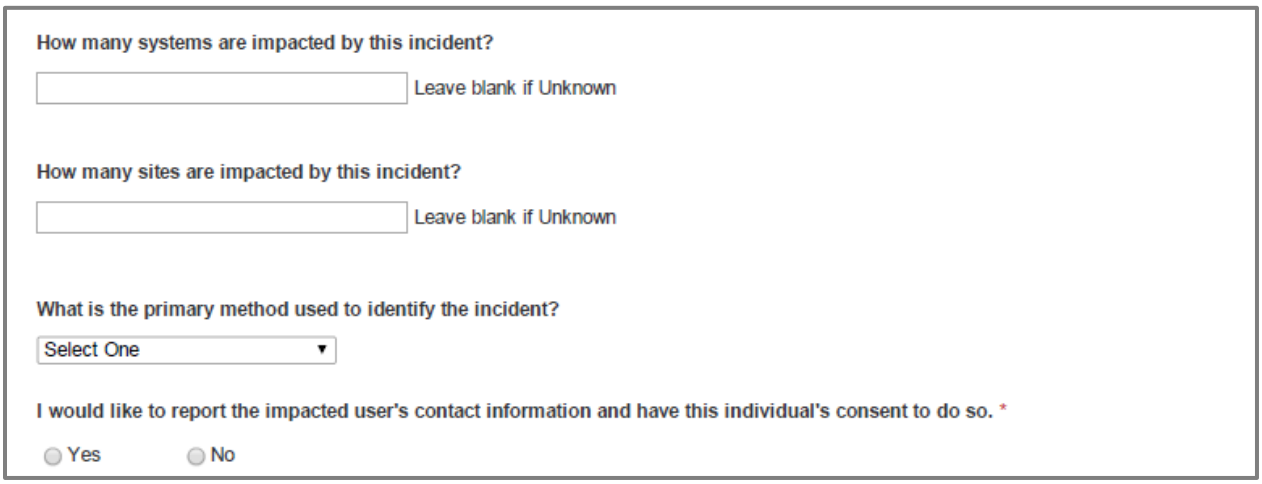
When was this incident detected?

Date E.g., 04/16/2015: 04/16/2015

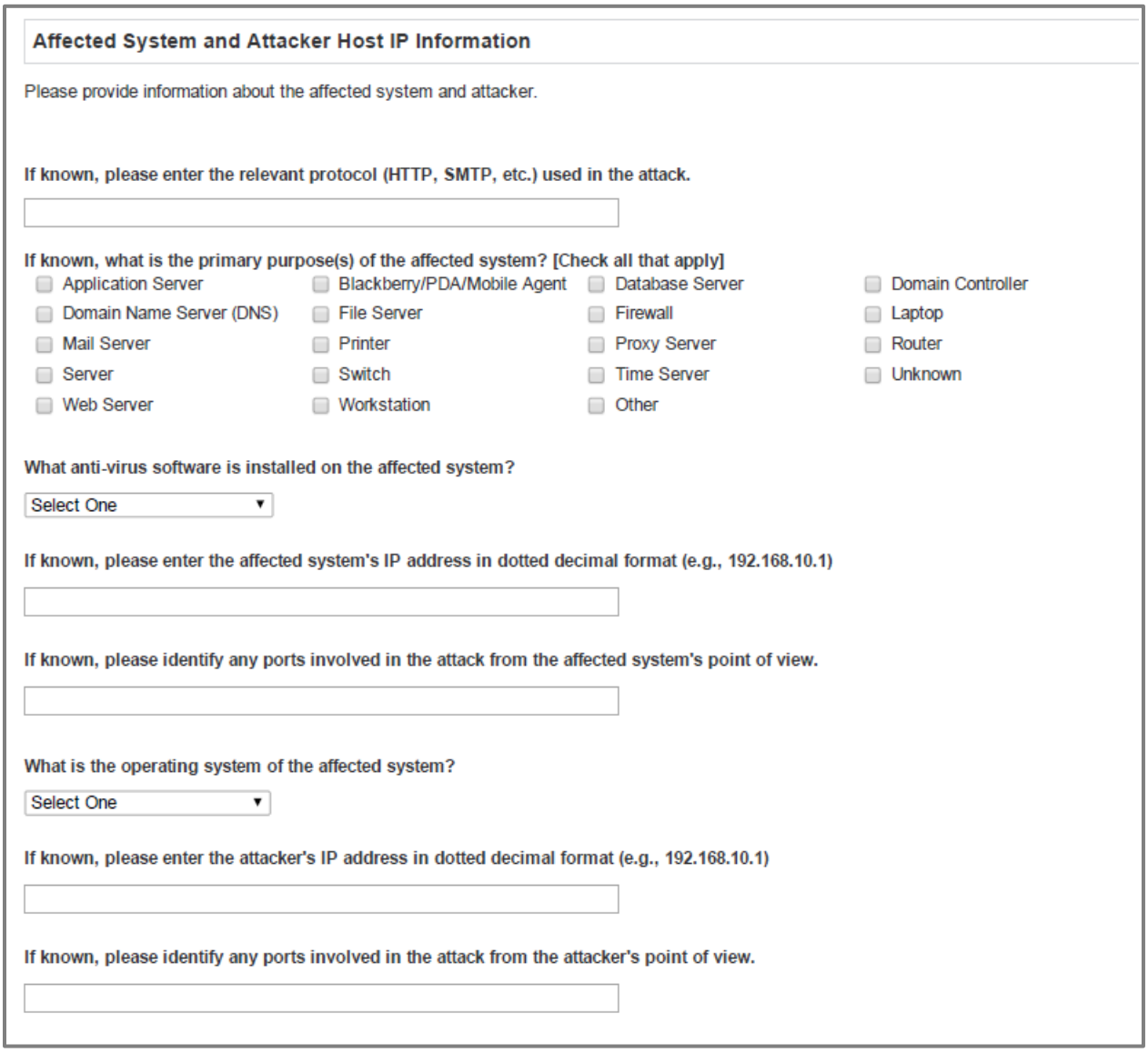
Time E.g., 11:36 AM: 11:36 AM

US-CERT Incident Reporting System





The following screen seeks to identify background information of the Affected and Attacker systems in breaches that are cybersecurity related in nature. As a reminder, breaches that are not cybersecurity related (i.e., paper) should not be reported to US-CERT.



Affected System and Attacker Host IP Information

Please provide information about the affected system and attacker.

If known, please enter the relevant protocol (HTTP, SMTP, etc.) used in the attack.

If known, what is the primary purpose(s) of the affected system? [Check all that apply]

- Application Server
- Blackberry/PDA/Mobile Agent
- Database Server
- Domain Controller
- Domain Name Server (DNS)
- File Server
- Firewall
- Laptop
- Mail Server
- Printer
- Proxy Server
- Router
- Server
- Switch
- Time Server
- Unknown
- Web Server
- Workstation
- Other

What anti-virus software is installed on the affected system?

Select One

If known, please enter the affected system's IP address in dotted decimal format (e.g., 192.168.10.1)

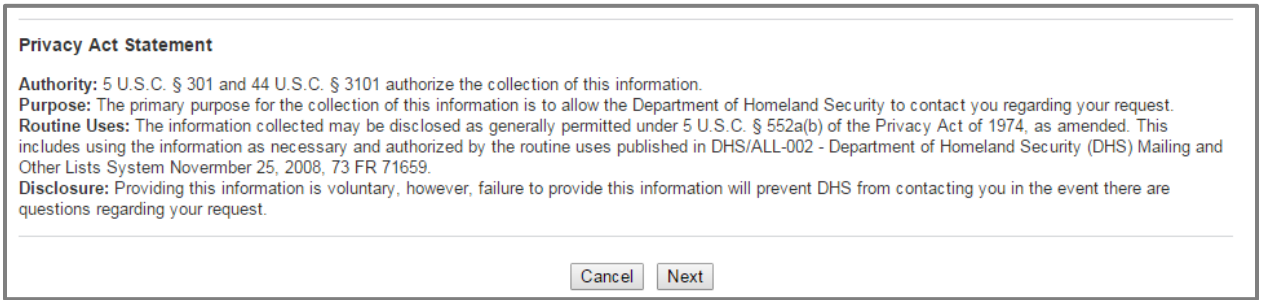
If known, please identify any ports involved in the attack from the affected system's point of view.

What is the operating system of the affected system?

Select One

If known, please enter the attacker's IP address in dotted decimal format (e.g., 192.168.10.1)

If known, please identify any ports involved in the attack from the attacker's point of view.



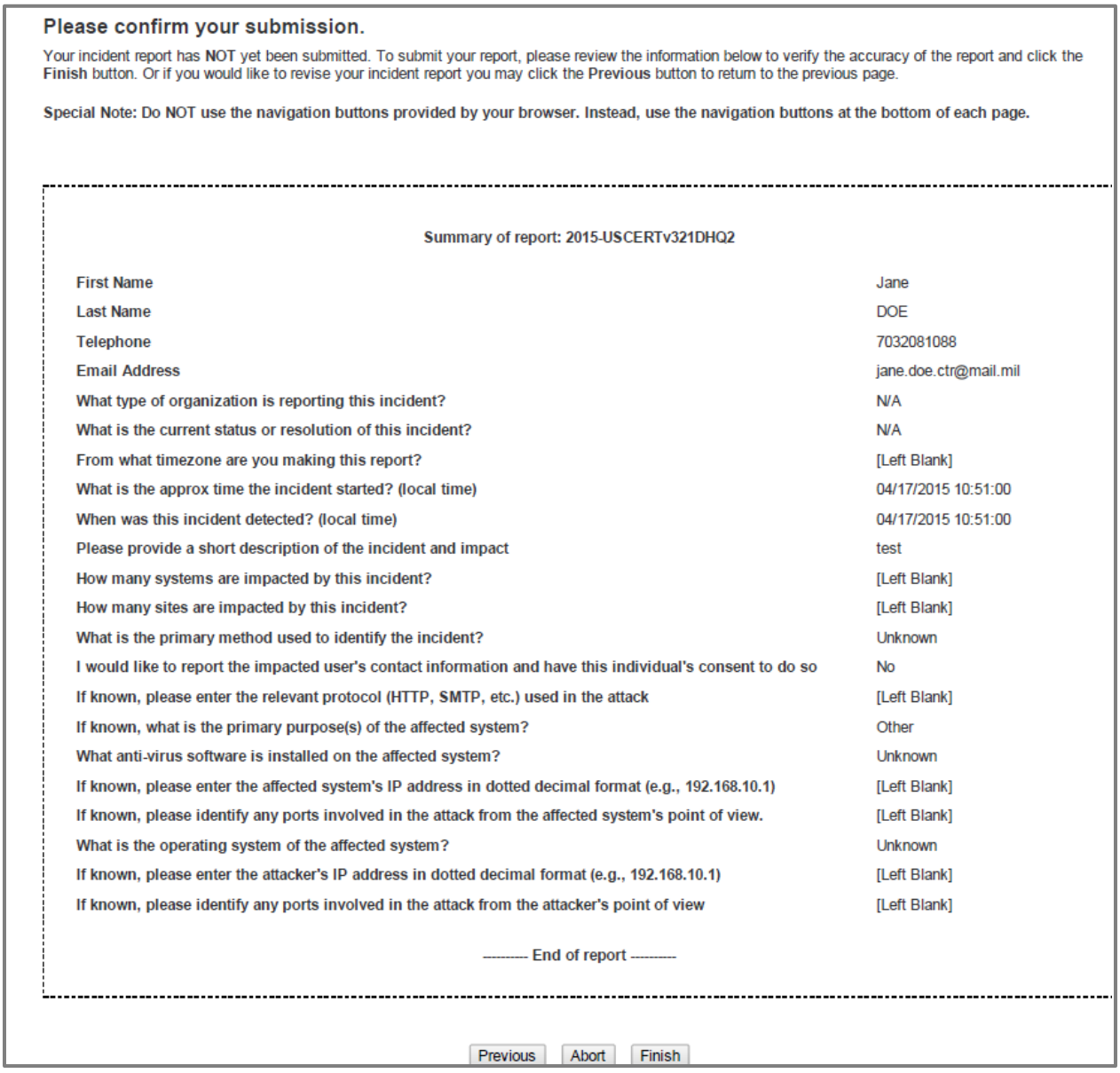
Privacy Act Statement

Authority: 5 U.S.C. § 301 and 44 U.S.C. § 3101 authorize the collection of this information.
Purpose: The primary purpose for the collection of this information is to allow the Department of Homeland Security to contact you regarding 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 Novermber 25, 2008, 73 FR 71659.
Disclosure: Providing this information is voluntary, however, failure to provide this information will prevent DHS from contacting you in the event there are questions regarding your request.

Cancel Next

Once these fields have been populated (or leave blank if not applicable), the US-CERT reporting is ready to be submitted. By clicking “Next” at the bottom of the screen, the user is routed to the following screen, which shows a summary of the report.

US-CERT Incident Reporting System



Please confirm your submission.

Your incident report has **NOT** yet been submitted. To submit your report, please review the information below to verify the accuracy of the report and click the **Finish** button. Or if you would like to revise your incident report you may click the **Previous** button to return to the previous page.

Special Note: Do NOT use the navigation buttons provided by your browser. Instead, use the navigation buttons at the bottom of each page.

Summary of report: 2015-USCERTv321DHQ2

First Name	Jane
Last Name	DOE
Telephone	7032081088
Email Address	jane.doe.ctr@mail.mil
What type of organization is reporting this incident?	N/A
What is the current status or resolution of this incident?	N/A
From what timezone are you making this report?	[Left Blank]
What is the approx time the incident started? (local time)	04/17/2015 10:51:00
When was this incident detected? (local time)	04/17/2015 10:51:00
Please provide a short description of the incident and impact	test
How many systems are impacted by this incident?	[Left Blank]
How many sites are impacted by this incident?	[Left Blank]
What is the primary method used to identify the incident?	Unknown
I would like to report the impacted user's contact information and have this individual's consent to do so	No
If known, please enter the relevant protocol (HTTP, SMTP, etc.) used in the attack	[Left Blank]
If known, what is the primary purpose(s) of the affected system?	Other
What anti-virus software is installed on the affected system?	Unknown
If known, please enter the affected system's IP address in dotted decimal format (e.g., 192.168.10.1)	[Left Blank]
If known, please identify any ports involved in the attack from the affected system's point of view.	[Left Blank]
What is the operating system of the affected system?	Unknown
If known, please enter the attacker's IP address in dotted decimal format (e.g., 192.168.10.1)	[Left Blank]
If known, please identify any ports involved in the attack from the attacker's point of view	[Left Blank]

--------- End of report ---------

Previous Abort Finish

This screen will provide the user with an opportunity to verify previous input for correctness. Once verified, clicking “Finish” will submit the report and will also generate a unique US-CERT number.

NOTE: It is critical for the user to record the US-CERT number assigned to the breach for accurate recordkeeping and for fulfilling additional breach reporting requirements.

As a reminder, any updates to the initial report are to be provided via email to soc@us-cert.gov and the assigned US-CERT number must be referenced in the subject line.