OPM Sensitive Information Loss Reporting Form

OPM Form 5084 v.3.2

Please fill out the information below and email this form to Cybersolutions@opm.gov as an attachment. Items with a * are mandatory fields. Instructions on the information for each field can be found starting on page 5 of this document.

As per the Carrier Letter, any loss must be reported to OPM within 30 minutes, but in no case later than 24 hours after identifying information loss.

Contact Details

1. **Contract Number*:**
   **Select 'Other" and type in if not available in dropdown.*
2. **Carrier – Legal Entity Name*:**
   **Type in name if contract number is not available.*
3. **Plan Name*:**
   **Type in name if contract number is not available.*
4. **Reporter's Name*:**
5. **Reporter's Email Address:**

Event Details*

6. **Date / Time of Compromise*:**
7. **Date / Time of Detection*:**
8. **Date / Time of CISA Notification*:**
   Type "Not Applicable" *if not reported to CISA*
9. **CISA Ticket Number:** ***skip if above is Not Applicable***
10. **Sensitive Information Type Lost***
11. **Current Incident Status***
12. **Country of Incident*:**
13. **Data Encrypted?*:**
14. **Source of Compromise*:**
15. **Attack Vector*:**
16. **Number of Systems Impacted*:**
17. **Incident Involved Criminal Activity?*:**
18. **Police Report Number** ***skip if above is No***

19. **Sensitive Information Lost***

Check all that apply. Include the number of records and users impacted for each type lost.	# of Records Impacted	# of Users Impacted
☐ Names, Address, Phone Numbers (with other elements present)	________	________
☐ D.O.B (or age)	________	________
☐ Credit / Debit Card Numbers	________	________
☐ Bank/Other Financial Acct. Info	________	________
☐ Login Credentials	________	________
☐ Misc. Background Case Info	________	________
☐ S.S.N	________	________
☐ Tax ID	________	________
☐ Medical Record Info	________	________
☐ Driver's License Number	________	________
☐ CSA/CSF Number	________	________
☐ Educational Info	________	________
☐ UEI/DUNS Number	________	________
☐ Evaluation	________	________
☐ Other	________	________
Totals	0	0

20. **Incident Severity*:**

21. **Explain the events leading to the loss of sensitive information.***

Include what happened, how PII was exposed, and how the loss may be prevented in the future.

22. **Describe the immediate actions taken.***

Include the actions that were taken to contain, mitigate, or recover the lost sensitive information.

Additional Reporting Details

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

   ☐ Yes ☐ No

2. **Add any Indicators of Compromise (IOCs) discovered.**

   IP Addresses, domains, malware hashes

System Impact

3. **Functional Impact:**
4. **Function of Affected Systems**

   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)
☐ Firewalls(s)
☐ ICS/SCADA System(s)
☐ Mail Server(s)
☐ Routers(s)
☐ Switch(es)
☐ Time Server(s)
☐ Web Server(s)
☐ Laptop(s)
☐ Other Server(s)

Observed Activity

5. **Location of Observed Activity:**
6. **Observed Activity Characterization:**

Impact Information

7. **Known Informational Impact:**

Recovery From Incident

8. **Organization Recoverability:**

9. **Estimated Impact Duration/ Recovery Timeline:**

10. **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

Please provide digital signature below*

By signing this document, you confirm that the information filled out on this form will be used, as is, in any reporting completed by the Office of Personnel Management and its staff.

Form Instructions

As per the Carrier Letter, any loss must be reported to OPM within 30 minutes, but in no case later than 24 hours after identifying information loss.

Contact Details

1. Contract Number: Select the contract number reporting from. Scroll to the bottom and select "Other" your number is not available on the list. This is a mandatory field.
2. Carrier – Legal Entity Name: Selected based off of Contract Number. Enter the name in the box if Contract Number was "Other". This is a mandatory field.
3. Plan Name: Selected based off of Contract Number. Enter the name in the box if Contract Number was "Other". This is a mandatory field.
4. Reporter's Name: Enter name of individual reporting the sensitive information loss. This is a mandatory field.
5. Reporter's Email Address: Enter email address of individual reporting the sensitive information loss.

Event Details

Use the drop-down to indicate if this is an initial, updated, or final report. This is a mandatory field. If it is an updated or final report, enter the ticket number provided by CyberSolutions. In the **Previous Report Ticket Number** field. (Example ADO **500500**)

6. Date / Time of Compromise: Enter approximate date and time the sensitive information loss initially occurred. This is a mandatory field.
7. Date / Time of Detection: Enter approximate date and time that the sensitive information loss was detected. This is a mandatory field.
8. Date / Time of CISA Notification: Enter approximate date and time the sensitive information loss was reported to CISA. Enter *"Not Applicable"* if loss was not reported to CISA. This is a mandatory field.
9. CISA Ticket Number: Enter the ticket number received when reported to CISA. Skip if "*Not Applicable*" was entered in number 8.
10. Sensitive Information Type Lost: Select appropriate drop-down option. This is a mandatory field.
    a. PII – Personal Identifying Information was lost.
    b. PHI – Personal Health Information was lost.
    c. Both – Both types of information were lost.
11. Current Incident Status: Select appropriate drop-down option. This is a mandatory field.
12. Country of Incident: Enter the country in which sensitive information loss occurred. This is a mandatory field.
13. Data Encrypted?: Choose the appropriate drop-down option. This is a mandatory field.
    a. Yes - if sensitive information was lost on an encrypted device (laptop requiring PIV, encrypted email, etc.)
    b. No - if sensitive information was lost on an unencrypted device (paper files, email, etc.)
    c. Unknown - if unsure of encryption status.

14. Source of Compromise: Select appropriate drop-down option. This is a mandatory field.
15. Attack Vector: Select the appropriate attack vector based off of CISA's Attack Vector descriptions. This is a mandatory field.
    a. https://www.cisa.gov/federal-incident-notification-guidelines#attack-vectors-taxonomy
16. Number of Systems Impacted: Enter number of known items impacted. This is a mandatory field.
17. Incident Involved Criminal Activity? – Choose appropriate drop-down option.
    a. No – criminal activity was not involved.
    b. Yes – criminal activity was involved.
18. Police Report Number: Enter police report number only if Yes selected for #17.
19. Sensitive Information Lost: Check all boxes that correspond to the types of sensitive information lost. Include the number of records and users impacted by the loss beside each checked item.
20. Incident Severity: Select the drop-down for the range related to the number of total records lost from item # 19. This is a mandatory field.
21. Explain the events leading to the loss of sensitive information: Provide details that lead to the loss of sensitive information. Include what happened, how PII was exposed, and how the loss may be prevented in the future.
22. Describe the immediate actions take: Provide the details of the actions taken to contain, mitigate, or recover the lost sensitive information. This is a mandatory field.

Additional Reporting Details

Use this section if the sensitive information loss was the result of a cybersecurity incident or breach.

1. Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised?: Select yes or no as appropriate.
2. Add any Indicators of Compromise (IOCs) discovered: Add any IOCs that were discovered during the investigation of the incident. This can include IP addresses, domains, hashes, program names or code snippets.

System Impact

3. Functional Impact: Select the impact of this loss from the dropdown based off CISA's impact category descriptions.
    a. https://www.cisa.gov/uscert/incident-notification-guidelines#impact-category-descriptions
4. Function of Affected Systems: Check all boxes that correspond to the functions of the affected systems.

Observed Activity

5. Location of Observed Activity: Select the appropriate dropdown option.
6. Observed Activity Characterization: Select the appropriate dropdown option.

Impact Information

7. Known Informational Impact: Select the appropriate dropdown option.

Recover From Incident

8. Organization Recoverability: Select the appropriate dropdown option.
9. Estimated Impact duration/Recovery Timeline: Include the amount of time systems will be impacted or the estimated time to recover from the cybersecurity incident or breach.
10. Does your agency currently consider this to be a breach that must be reported to Congress within 30 days in accordance with OMB Policy?: Select yes or no as appropriate.

Please provide a digital signature on the form. This will confirm that the information provided by the reporter can be used, as is, in any reporting completed by the Office of Personnel Management and its staff, as well as help to preserve the integrity of the report. This is a mandatory field.