



US Department of Agriculture

Agriculture Security Operations Center

Cyber Security Incident Report

Personally Identifiable Information (PII) Incident

This Cyber Security Incident Report follows established guidelines as determined in Departmental Manual 3505-001: USDA Cyber Security Incident Handling Procedures, Appendix A and US-CERT Federal Incident Notification Guidelines of 2014

[https://www.us-cert.gov/sites/default/files/publications/Federal Incident Notification Guidelines.pdf](https://www.us-cert.gov/sites/default/files/publications/Federal%20Incident%20Notification%20Guidelines.pdf).

Complete the sections identified for the appropriate US-CERT Category within 30 days of incident discovery.

Category 1 – Unauthorized Access

[Section I: General Information](#)

[Section II A: Incident Mitigation – Category 1 – Unauthorized Access](#)

[Section III: Impact and Scope](#)

[Section IV: Lessons Learned](#)

[Section V: Additional Information](#)

Category 8 – Lost/Stolen Equipment

[Section I: General Information](#)

[Section II B: Incident Mitigation – Category 8 – Lost/Stolen Equipment](#)

[Section III: Impact and Scope](#)

[Section IV: Lessons Learned](#)

[Section V: Additional Information](#)

ASOC PII Incident Report

Please send all updates, information and reports for this incident to cyber.incidents@asoc.usda.gov or contact the ASOC via the 24-hour Cyber Incidents Hotline (866) 905-6890.

Section I: General Information

| A. Agency Information | |
|---|--|
| ASOC Incident Number: | <<OIS Provided, if applicable>> |
| Agency Incident Number: | <<RMA Provided>> |
| Reporting Individual and Organization Submitting this Report: | <<RMA Provided>> |
| Date: | <<RMA Provided>> |
| Impacted Organization and individual contacted, if applicable: | <<Only fill out if RMA or OIS information security monitoring measures indicate compromise at AIP and we notify them>> |
| Date and time, including Time Zone, that impacted organization was notified, if applicable: | <<RMA fills out based on alert>> |
| B. ISSPM/CISO Contact | |
| Name of ISSPM or CISO: | |
| Position/Title: | |
| E-Mail Address: | |
| Office Phone: | 816-926-3306 |
| Cell Phone: | 816-469-9269 |
| C. Privacy Officer Contact | |
| Name of Privacy Officer Point of Contact: | |
| Position/Title: | |
| E-Mail Address: | |
| Office Phone: | |
| Cell Phone: | |
| Agency Privacy Officer Notification Date: | <<RMA fills out upon notification>> |
| D. Person Assigned to Investigate | |
| Name of Investigative Point of Contact: | |
| Position/Title: | |
| E-Mail Address: | |
| Office Phone: | |
| Cell Phone: | |

ASOC PII Incident Report

| E. Reporter Information | |
|---|---------------------|
| Name of Individual who reported PII exposure: | <<Provided by AIP>> |
| Position/Title: | <<Provided by AIP>> |
| E-Mail: | <<Provided by AIP>> |
| Office Phone: | <<Provided by AIP>> |
| Cell Phone: | <<Provided by AIP>> |
| F. Other Contact Information | |
| Name of Individual who exposed the PII: | <<Provided by AIP>> |
| Position/Title: | <<Provided by AIP>> |
| E-Mail: | <<Provided by AIP>> |
| Office Phone: | <<Provided by AIP>> |
| Cell Phone: | <<Provided by AIP>> |
| G. General Information | |
| How was the incident discovered, including sources, methods or tools used to identify the incident (IDS, Audit logs, Digital Media Analysis)? | <<Provided by AIP>> |
| Details describing any cyber vulnerabilities (CVE identifiers), if applicable: | <<Provided by AIP>> |
| Date/Time of the occurrence, including time zone: | <<Provided by AIP>> |
| Date/Time of detection, including time zone: | <<Provided by AIP>> |
| Date/Time of identification, including time zone: | <<Provided by AIP>> |
| System Functions, if applicable (web server, domain controller, SharePoint, workstation): Operating System(s) affected, if applicable: | <<Provided by AIP>> |
| Physical System Location(s): | <<Provided by AIP>> |
| Source Internet Protocol (IP) address, port & protocol, if applicable: | <<Provided by AIP>> |
| Destination Internet Protocol (IP) address, port & protocol, if applicable: | <<Provided by AIP>> |
| Type of Media (i.e. paper based, laptop, other electronic media [CD, DVD, USB], website posting, PDA, E-Mail, SharePoint): | <<Provided by AIP>> |
| If non-Cyber, US-CERT shall not be notified. Date and time agency/staff office PO/PAO was notified: | <<Provided by AIP>> |

ASOC PII Incident Report

| | |
|---|--|
| <p>If paper based, were the documents double wrapped? If the answer is no, why were the documents not double wrapped?</p> | <p><<Provided by AIP>></p> |
| <p>If cyber-based PII exposure, was it the result of an attack? If yes, please identify if the attack was unknown, Attrition, Web-based, E-mail, External/Removable media, Impersonation/Spoofing, Improper Usage or Loss or Theft of Equipment. (If lost or stolen, please complete Section II, B.</p> | <p><<Provided by AIP>></p> |
| <p>Number of Individuals Affected:</p> | <p><<Provided by AIP>></p> |
| <p>Type of PII Exposed (i.e. SSN, Name, DOB, TIN, etc.):</p> | <p><<Provided by AIP>></p> |
| <p>Did this occur on a cloud-based system? If yes, is it a contractor cloud-based system?</p> | <p><<Provided by AIP>></p> |
| <p>Is there a Privacy Threshold Analysis (PTA)? (Every System Requires a PTA.) If not assigned to a system, please explain the reasons for the collection and use of the PII.</p> | |
| <p>If yes, enter the date signed by the agency CIO/Official. If no, explain reason for no PTA.</p> | |
| <p>Is there a Privacy Impact Assessment (PIA)?</p> | |
| <p>If yes, enter the date signed by the agency CIO/Official. If no, explain reason for no PIA.</p> | |
| <p>What is the General Support System (GSS) on which this application or PII is process/stored?</p> | |
| <p>Enter the name(s) of the SORN(s).</p> | |
| <p>Enter the Federal Register System of Record Notification (SORN) number, publication date, volume and page number(s), if applicable. Date that the SORN was uploaded to the Federal Register.</p> | |
| <p>Enter date and Electronic Correspondence Management (ECM) control number.</p> | |
| <p>Please enter the Authority to Operate (ATO) date.</p> | |
| <p>Are there any open POA&Ms for the system?</p> | |

ASOC PII Incident Report

| | |
|---|---------------------|
| If so, please enter the POA&M number: | |
| Is there a signed Computer Matching Agreement (CMA) or Interconnection Security Agreement (ISA) with the agency which the information was matched or shared? List the effective date. | |
| Was the CMA approved by the Data Integrity Board? If yes, please document the date of approval. | |
| Was the PII extracted/downloaded from a database? | <<Provided by AIP>> |
| If yes, was the extraction/download logged as required by: M-07-16? Describe process for logging extractions. Who is responsible for logging and tracking the extraction? | <<Provided by AIP>> |

Section II: Incident Mitigation

| A. Category 1 – Unauthorized Access | |
|--|---------------------|
| Circumstances surrounding the incident: | <<Provided by AIP>> |
| Mitigating Factors (full disk encryption, complex passwords, PIV card access): | <<Provided by AIP>> |
| Describe steps taken to contain and mitigate this incident. | <<Provided by AIP>> |
| Has the individual(s) responsible for the breach/exposure/incident completed annual information security awareness training? If not, why not? | <<Provided by AIP>> |
| Was (were) the individual(s) responsible for breaching the PII notified and counseled about protecting PII prior to the breach? | <<Provided by AIP>> |
| Has the individual(s) responsible for exposing the PII completed the PII training in AgLearn? If yes, attach the certificate of completion or enter the documented date of completion. | |
| Does your agency have Rules of Conduct as required by OMB Memorandum M-07-16 that incorporate USDA privacy requirements? Does your agency ensure that all individuals who are authorized to access PII and their supervisors sign, at least annually, a document that clearly describes their responsibilities? | |

ASOC PII Incident Report

| | |
|---|--|
| <p>If it does not, how are users reminded of their responsibilities to protect PII?</p> | |
| <p>If yes, was the person responsible for breaching/exposing the PII aware of those rules? If unaware, explain and have the person read and sign and date the Rules of Behavior. Please include a copy of the receipt or verify date of signature in the final submission of this form.</p> | |
| <p>If the incident was facilitated by e-mail, does your organization provide encryption and/or password protection for e-mail attachments? If yes, was the person who compromised the PII aware of her/his responsibility to encrypt or password protect the PII before sending? If yes, why was it not done? If no, will your policies and procedures be modified to require encryption/password protection?</p> | <p style="background-color: yellow;"><<Provided by AIP>></p> |
| <p>Was there any indication of criminal activity? If yes, provide date(s) and case number(s) of OIG/Law Enforcement notification. Please attach or provide the number of the police/OIG report or case number (if releasable)</p> | <p style="background-color: yellow;"><<Provided by AIP>></p> |
| <p>Were the impacted individuals Notified?</p> | <p style="background-color: yellow;"><<Provided by AIP>></p> |
| <p>If the individuals were notified, how many were Notified?</p> | <p style="background-color: yellow;"><<Provided by AIP>></p> |
| <p>Was credit monitoring offered to the individual(s) impacted by the PII exposure? If yes, please submit a copy of the approved offer letter along with the date it was sent. If no, please explain.</p> | <p style="background-color: yellow;"><<Provided by AIP>></p> |
| <p>Was a signed non-disclosure statement (AD – 3050) received from all individual(s) who viewed the PII? www.ocio.usda.gov/document/ad-3050 If yes, please submit copies of the non-disclosure document(s). If no, please explain.</p> | |

ASOC PII Incident Report

| B. Category 1 (US-CERT CAT 1) - Lost/Stolen Equipment Containing PII | |
|--|---------------------|
| Type(s) of USDA issued equipment (i.e. make, model, serial number, phone number): | |
| Approximate replacement value: | |
| Address/Location where the incident occurred: | <<Provided by AIP>> |
| Circumstances surrounding the incident: | <<Provided by AIP>> |
| Was the individual authorized to remove the device(s) from the USDA duty station? If yes, is there a signed property pass? If yes, did it include rules of use, conduct and behavior? If no, why is there no property pass? | |
| Was encryption software installed? If yes, what version? If not, please state why it is not installed. | <<Provided by AIP>> |
| Was the equipment/device(s) password protected? Please answer for each device. | <<Provided by AIP>> |
| Has the service or network access been disabled? | <<Provided by AIP>> |
| If the equipment was a mobile device (i.e. Smartphone, tablet, etc.) was it remotely purged? If no, explain. | <<Provided by AIP>> |
| If stolen, what law enforcement agency was notified? List the police report number, date and name of investigating officer. | <<Provided by AIP>> |
| If lost, what actions were taken to find the equipment? | <<Provided by AIP>> |
| Was the individual(s) responsible for the lost or stolen equipment trained to protect the equipment from loss or theft? | <<Provided by AIP>> |
| Were any of the devices lost or stolen containing USDA PII personally owned (non-USDA issued) such as: thumbdrive, portable hard drive? If Yes, please document why PII was resident on personally owned equipment. | |

Section III: Impact and Scope (To Be Filled out by RMA)

A. Impact and Scope

ASOC PII Incident Report

| | |
|--|---|
| <p>Determine the FIPS 199 Security Categorization (SC) to determine potential impact levels. This applies to systems used by or on behalf of USDA. All systems must be categorized.</p> | <p>Confidentiality: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High <input type="checkbox"/> N/A</p> <p>Integrity: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High <input type="checkbox"/>N/A</p> <p>Availability: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High <input type="checkbox"/>N/A</p> <p>Explain Not Applicable (N/A) Responses:</p> |
| <p>Summary of FIPS 199 Security Categorization (SC) of for the system that contains the PII.</p> | <p><input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High <input type="checkbox"/>N/A</p> |
| <p>Determine the NIST 800-122 Confidentiality Impact Level based on the NIST 800-122 Factors.</p> | <p>Identifiability: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High <input type="checkbox"/>N/A</p> <p>Quantity of PII: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High <input type="checkbox"/>N/A (< 500) (500-1000) (> 1000)</p> <p>Data Field Sensitivity: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High <input type="checkbox"/>N/A</p> <p>Context of Use: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High <input type="checkbox"/>N/A</p> <p>Obligation to Protect Confidentiality: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High <input type="checkbox"/>N/A</p> <p>Access to and Location of PII: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High <input type="checkbox"/>N/A</p> |
| <p>Combined NIST 800-122 Confidentiality Impact Level.</p> | <p><input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High <input type="checkbox"/>N/A</p> |
| <p>Explain the rationale for the combined NIST 800-122 Confidentiality Impact Level. Note: This combined impact level contributes to the determination of the overall incident category.</p> | |
| <p>Determine the OMB M-07-16 Risk factors to assess the likely risk of harm stemming from the breach of PII.</p> | <p>Nature of Data Elements: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High</p> <p>Likelihood the PII is Usable: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High</p> <p>Likelihood PII May Lead to Harm: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High</p> <p>Ability to Mitigate the Risk of Harm: <input type="checkbox"/>Low <input type="checkbox"/>Moderate <input type="checkbox"/>High</p> <p>Actual Number of Individuals Affected: (Should be answered in Section I, Subsection G. above unless the number has changed due to the investigation.)</p> |
| <p>US-CERT Impact Classifications</p> | |

ASOC PII Incident Report

| | |
|---|--|
| <p>Functional Impact: HIGH – Organization has lost the ability to provide all critical services to all system users. MEDIUM – Organization has lost the ability to provide a critical service to a subset of system users. LOW - Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance NONE - Organization has experienced no loss in ability to provide all services to all users.</p> | <input type="checkbox"/> None <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High |
| <p>Information Impact: PRIVACY – The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised. INTEGRITY – The necessary integrity of information was modified without authorization. NONE – No information was exfiltrated, modified, deleted or otherwise compromised.</p> | <input type="checkbox"/> None <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High <input type="checkbox"/> None <input type="checkbox"/> Low <input type="checkbox"/> Moderate <input type="checkbox"/> High |
| <p>Recoverability: REGULAR – Time to recovery is predictable with existing resources. SUPPLEMENTED – Time to recovery is predictable with additional resources. EXTENDED – Time to recovery is unpredictable, additional resources and outside help are needed. NOT RECOVERABLE- Recovery from the incident is not possible (Example, PII exfiltrated and posted publically). NOT APPLICABLE – Incident does not require recovery.</p> | <input type="checkbox"/> Regular <input type="checkbox"/> Supplemented <input type="checkbox"/> Extended <input type="checkbox"/> Not Recoverable <input type="checkbox"/> Not Applicable Please include narratives here: |

Section IV: Lessons Learned

| A. Lessons Learned | |
|--|--|
| How could this incident have been prevented? | |
| What additional information was required to investigate/resolve this incident? | |
| Where was this information available? | |
| What will your organization do to prevent further breaches? | |

ASOC PII Incident Report

| | |
|---|--|
| Are there any deficiencies in Departmental or Agency policies and procedures that would assist in preventing future breaches or exposures? (Please enter as much information as possible.) | |
|---|--|

Section V: Additional Information

Provide timelines, related documents, such as NITC service desk form, credit monitoring offer letters, non-disclosure forms, pertinent e-mail messages and any additional information not included in previous sections:
