



U.S. Department of Transportation
Privacy Impact Assessment
Office of Inspector General
OIG

Computer Crimes Unit Network
CCUNet

Responsible Official

Juana Sawi
oitprivacy@oit.dot.gov
202-366-2589

Reviewing Official

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

August 6, 2021





Executive Summary

The mission of the Office of Inspector General (OIG) is to ensure a safe, efficient, and effective transportation system and work within the Department of Transportation (DOT) to promote effectiveness and prevent or identify fraud, waste, and abuse in departmental programs. The OIG does this through audits and investigations. OIG also consults with the Congress about programs in progress and proposed new laws and regulations.

In its mission to ensure a safe, efficient, accessible, and convenient transportation system that meets our vital national interests and enhances the quality of life, OIG collects, accesses, and uses significant amounts of data every day. With increased data collection comes increased privacy risk to DOT employees, contractors, and members of the public. The OIG is committed to protecting the integrity and confidentiality of all data throughout all its component systems.

This purpose of this privacy impact assessment is to proactively document the risk management framework associated with the DOT/OIG Data Analytics and Computer Crimes Unit (DACC) Network (CCUNet) to ensure privacy of all data managed within the system. The system serves as a temporary workspace where OIG investigators can process and review evidence collected via a variety of sources such as subpoena, consent, or warrant directly supporting OIG investigations as authorized by the Inspector General Act of 1978. Such evidence may include any form of privacy information the person or business being investigated collected or maintained in any number of electronic formats. For example, a single forensic image acquired during a search warrant of a business may contain a database of personal information for customers of the business or detailed employee information. Since the scope of such evidence is very broad, the OIG DACC takes extreme precautions above and beyond what is mandated by federal regulations to ensure the privacy of the information is maintained.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii)



examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.¹

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use, and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- Accountability for privacy issues;*
- Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The United States Department of Transportation Office of the Inspector General (US DOT/OIG), Data Analytics and Computer Crimes Unit (DACC), Computer Crimes Unit Network (CCUNet) provides a means to process and analyze data in a comprehensive, accurate, and manageable manner to support various OIG investigations. CCUNet is considered a non-mission critical General Support System (GSS) according to the DOT General Support Systems and Major Application Certification and Accreditation Guide. CCUNet serves two primary purposes (1) to provide secure data analytics and forensic environments to process investigative case data and (2) to provide OIG case agents secured access to case data and the tools necessary to search and view that data.

The system contains data collected as part of OIG investigations including data obtained via consent, subpoena, search warrant as well as departmental data provided to the OIG from the various DOT modes. "Working copies" of the evidentiary data are created and verified on CCUNet forensic servers and then processed to separate out the innocuous computer files from the documentary evidence which is extracted and uploaded to either a case virtual machine or the NUIX² web review platform. This process then allows the specific case

¹Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

² NUIX is a proprietary off-the-shelf forensic tool that allows case agents to search, review and tag data for extraction or forensic reporting.



agent to index and search text-based evidence or view image-based evidence specific to the case (typically in compliance with any warrant limitations). Once key documents are identified by investigators, OIG CCU personnel write up forensic media analysis (FMA) reports to support investigative legal proceedings. The data within CCUNet is maintained and destroyed in accordance with established OIG evidence policy and procedures. For example, at the completion of legal proceedings, evidence working copies as well as the case virtual machine or NUIX case in CCUNet are destroyed. CCUNet is a temporary workspace containing only “working copies” of the electronic evidence or data and does not represent “records” created or maintained under federal regulations. Rather, the case agent reports, CCU forensic reports, data analytics reports and legal documentation created outside of the CCUNet system represent the official “records” and are maintained in other OIG systems such as the OIG investigations electronic case management system or the OIG Infrastructure.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3³, sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations⁴.

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization’s information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

CCUNet is a temporary workspace where duplicate “working copies” of case evidence is processed and reviewed. CCUNet is not a “system of records” nor does it contain any official records. Rather, electronic data is collected as part of the OIG investigative process

³ <http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf>

⁴ http://csrc.nist.gov/publications/drafts/800-53-Appendix-J/IPDraft_800-53-privacy-appendix-J.pdf



under the OIG Records System ([DOT/OST 100 - Investigative Record System](#) - 77 FR 42797 - July 20, 2012). This specifically includes “paper investigative files” as well as electronic records in the OIG Office of Investigations “electronic case management and tracking information system.” Thus, the electronic case management system is the official system of record where evidence is managed, and all official investigative reports are uploaded including forensics reports, field memos and other reports developed by the DACC. CCUNet is merely a separate workspace for duplicate “working copies” of evidence or departmental data.

While CCUNet is only a temporary workspace for evidence and contains no official records, electronic evidence collected or processed by the DACC in CCUNet often includes privacy information. For example, computer systems acquired as forensic images while executing a search warrant may include many types of privacy information on individuals such as customers or employees. CCUNet does not directly collect privacy information such as collecting personal information into a database. However, CCUNet security is based on the assumption that such privacy information will be present in the data collected (indirectly). The OIG DACC therefore maintains a level of security of the system equivalent to the risks associated with maintaining such data. As per any federal system, the specific security controls are documented within the system security plan and associated security package. Additionally, the risk of maintaining any such data accepted by senior level OIG executives who ensure the security of the system meets or exceeds the level required to mitigate associated risks.

As stated in the OIG Privacy Policy, the OIG builds public trust and acceptance through public notice of its information practices and the privacy impact of its programs and activities. Specifically, the OIG policy states that the OIG will:

- be transparent and provide notice to the individual regarding its collection, use, dissemination and maintenance of PII.
- maintain no system of records without first giving public notice through a SORN published in the Federal Register.
- publish a Privacy Act Exemption Rule (Exemption Rule) for any system of records it intends to exempt from portions of the Privacy Act.
- to the extent practical, make publically available its analysis of the privacy risks created by OIG information systems, programs or activities implemented through regulations, information collections and any implemented risk mitigation strategies. At a minimum, and to the extent permitted by law, the OIG will make publically available approved PIAs, SORNs, Exemption Rules, and reports developed or created in response to oversight bodies including the OMB, U.S. Congress and the Government Accountability Office (GAO).
- to the extent practical, make publically available its privacy practices, including but not limited to PIAs, SORNs and privacy reports.



- provide an online privacy policy explaining its privacy-related practices pertaining to its official external website and its other online activities.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Information in the CCUNet system is typically the result of the legal investigative process obtained under personal consent, subpoena, warrant or through other investigative evidence collecting procedures. Any such data is treated in accordance with evidentiary procedures. The Freedom of Information Act (FOIA) generally provides that any person has the right to request access to federal agency records or information except to the extent the records are protected from disclosure by any of nine exemptions contained in the law or by one of three special law enforcement record exclusions. Exemption 7(A), authorizes the withholding of "records or information compiled for law enforcement purposes, but only to the extent that production of such law enforcement records or information . . . could reasonably be expected to interfere with enforcement proceedings."⁵ As such, FOIA requests are evaluated on a case-by-case basis for any OIG investigative data.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

The OIG Office of Investigations is comprised of criminal and general investigators who are responsible for conducting criminal, civil, and administrative investigations of fraud and a variety of other allegations affecting DOT, its operating administrations, programs, and grantees. The legal basis and authority was established through the Inspector General's Act of 1978. Additionally, the Homeland Security Act of 2002 granted OIG Investigations special agents permanent statutory law enforcement authority including the authority to make arrests, obtain and execute search warrants and carry firearms. It is through this authority that the OIG collects information throughout the investigative process, typically by interview, consent, subpoena, or search warrant. Any information collected and

⁵ <https://www.justice.gov/oip/foia-guide-2004-edition-exemption-7a>



subsequently processed, stored, or provided to the OIG case agents as part of the CCUNet system is authorized for the specific purpose of conducting such investigations.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

Data is collected in accordance with legal proceedings such as warrant, subpoena or consent pursuant to the legal authority granted to OIG investigators. Privacy information within CCUNet is maintained and destroyed in accordance with evidentiary policy and procedures and retained only as necessary to support ongoing investigations. All “working copies” of original evidence, VMs, and data staged for processing within CCUNet for a case are destroyed at the same time as the original evidence at the conclusion or resolution of legal proceedings for a case. As there are no official records in the system, the National Archives and Records Administration (NARA) disposition schedule does not apply.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

As defined in the OIG Privacy Policy, OIG programs and information systems are restricted in the collection and use of PII, or activity impacting privacy, to that which is authorized by law. As such OIG will:

- determine the legal authority that permits its collection, use, maintenance and sharing of PII, either generally or in support of a specific program or information system need.
- clearly specify usage purposes within legal authorities.
- maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

The policy also defines the internal sharing of such data as follows:

- Unless otherwise limited by statute, information collected by a DOT Component will be considered an information asset of the entire Department.⁶

⁶ This provision should not be construed as a basis for limiting or denying the Office of Inspector General access to PII that they are otherwise authorized to obtain.



- Unless explicitly authorized or mandated by law, OIG will permit internal sharing of PII only for a purpose compatible with the original purpose of collection, specified at the time of initial collection.
- OIG will document all authorized internal sharing of PII via a Memorandum of Understanding (MOU) or other approved instrument that articulates the conditions of access and use.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

Data obtained and maintained in the CCUNet system exists as a working copy of the original evidence and its accuracy will be determined in one of several ways, including verification by the case agent through the investigative process or by forensic verification through the DACC Forensic Media Analysis (FMA) reporting process.

In accordance with OIG policy and procedure, information shall be sufficiently accurate, complete, and up to date to minimize the possibility that inappropriate information may be used to make a decision about an individual.

Additionally, OIG will:

- make reasonable efforts, prior to disseminating a record about an individual, to ensure that the record is accurate, relevant, timely and complete.
- to the extent feasible, establish mechanisms to allow individuals to access and correct information about them.
- develop and implement reasonable procedures to ensure the accuracy of the data shared and the data received.
- investigate alleged errors or deficiencies in PII that has been shared in a timely manner and will correct, delete or not use the PII if found to be inaccurate.
- take timely, appropriate steps to provide written notice to the recipient of the shared data regarding any errors identified and request that the inaccurate PII be corrected or deleted.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.



CCUNet is a fully certified and accredited General Support System (GSS) supporting the mission of the OIG DACC and is categorized with an overall risk rating of “Moderate” in accordance with Federal Information Processing Standards (FIPS) Publication (PUB) 199, Standards for Security Categorization of Federal Information and Information Systems; and NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems. Privacy information collected as evidence and duplicated within CCUNet is protected in accordance with the system security plan. Access to all systems requires users to accept the “banner” acknowledging the proper use, access, and rights to the system. In addition, all users must sign CCUNet “Rules of Behavior” (ROBs) prior to access as well as annually which delineates specific handling of PII/SPII in accordance with approved OIG policy and procedures.

Privacy information can exist in CCUNet in multiple locations including the forensic and data analytics processing servers, case-specific virtual machines and the NUIX Web Review back end server. The OIG DACC takes extreme care in ensuring the security of this data by applying controls that meet or exceed the baseline criteria for federal information processing systems designated by NIST and the Federal Information Security Management Act (FISMA). Examples of such controls include the requirement to access the aforementioned servers and VMs using PIV smart cards with the control set at the “machine level.” This means that no access is provided without a valid smart card authentication. Additionally, the forensic servers employ additional controls that further limit access, such as Network Level Authentication⁷ (NLA) and IPsec⁸.

Access to VMs is limited to only CCU employees and the specific case agent or agents assigned to the machine on a need to know basis. All drives potentially hosting privacy data are encrypted, including both the operating system and data drives. Additionally, all network traffic to or from the OIG client machines with VMs and application servers is encrypted using IPsec. All systems are monitored daily for configuration changes and system events of critical servers are monitored in real-time to identify specific threats to the system. Complete documentation is available via the Departmental Cyber Security Assessment and Management System (CSAM).

⁷ Network Level Authentication is a technology used in Remote Desktop Services (RDP Server) or Remote Desktop Connection (RDP Client) that requires the connecting user to authenticate themselves before a session is established with the server. Reference: https://en.wikipedia.org/wiki/Network_Level_Authentication

⁸ Internet Protocol security (IPsec) is a framework of open standards for helping to ensure private, secure communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPsec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. Because IPsec is integrated at the Internet layer (layer 3), it provides security for almost all protocols in the TCP/IP suite, and because IPsec is applied transparently to applications, there is no need to configure separate security for each application that uses TCP/IP. Reference: [https://technet.microsoft.com/en-us/library/cc776369\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc776369(v=ws.10).aspx)



Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

Being a fully certified and accredited system means that CCUNet must adhere to stringent reporting and auditing to ensure the system effectively implements controls to protect the system from risks and to ensure any remaining risk is accepted by the authorizing official. CCUNet employs controls to ensure any threats, suspicious activity, or changes to the system posture are continuously monitored. As detailed in the CCUNet *Continuous Monitoring Plan*, security monitoring includes asset discovery and management, vulnerability assessment, configuration compliance, event log monitoring and account monitoring. Each of those areas are stringently monitored and audited for compliance starting with system baselines which are based on security control settings developed by the Center for Internet Security (CIS). CCUNet is setup to report the status of baseline controls daily including a summary of controls for every system in CCUNet that is emailed daily to the CCUNet system administrators. Additionally, CCUNet employs controls to audit and monitor the state of the system based on the following schedule:

- System auditing: Real time with operating system advanced auditing settings and real time notifications
- Vulnerability Assessment and Management: Daily scans of all systems
- Systems Patch Management: Daily with summary reports emailed directly to system administrators
- Configuration Compliance Management: Daily based on CIS baselines
- Expired Account Monitoring: Daily
- Account Monitoring: Detected in real-time with event log and group monitoring tools
- Group Monitoring: Real time and daily using multiple tools
- Security Event Monitoring: Real-time with direct email notifications for specific events
- Enforcement of Controls review: Annually including FISMA reporting
- Plan of Action and Milestone update: Quarterly
- Unauthorized software detection: Daily and at system boot.
- Incident response capability: Annually
- Risk Assessment: Annually and/or with major change to the system.

CCUNet has also been directly audited by the US DOT/OIG Auditors for the past five years for FISMA compliance and audited by the same group in 2016 for compliance with the



Cybersecurity Act of 2015. CCUNet was also independently assessed by the Federal Aviation Administration (FAA) Electronic Services Center (ESC) each year since 2017 for FISMA control compliance. Such continuous monitoring and independent scrutiny ensures CCUNet provides adequate protection of system data including PII and SPII.

Responsible Official

Juana Sawi
Information Systems Security Manager

Approval and Signature

Karyn Gorman
Acting Chief Privacy Officer
Office of the Chief Information Officer

