Privacy Impact Assessment

for the

Classified Data Forensics Workstation (CDFW)

DHS Reference No. DHS/OIG/PIA-005

October 2, 2024

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) is responsible for conducting and supervising independent and objective audits, inspections, and investigations of DHS's programs and operations. The DHS OIG Office of Investigations (INV) will operate a stand-alone Classified Data Forensics Workstation (CDFW) to assist with OIG's investigative mission. The CDFW will process electronically stored information (ESI) obtained from digital evidence devices (e.g., electronic devices, USB/thumb drives, CDs/DVDs) acquired as part of active investigations of alleged criminal, civil, or administrative violations by DHS employees, contractors, grantees, beneficiaries, and other individuals and entities associated with DHS. OIG conducted this Privacy Impact Assessment (PIA) because the data that may be obtained and processed from digital evidence devices may consist of personally identifiable information (PII) and/or sensitive personally identifiable information (SPII).

Overview

Under the Inspector General Act of 1978, as amended,[1] DHS OIG is responsible for conducting and supervising independent and objective audits, inspections, and investigations of the programs and operations of DHS. OIG promotes economy, efficiency, and effectiveness within the Department and prevents and detects employee corruption, fraud, waste, and abuse in its programs and operations. OIG's Office of Investigations investigates allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, grantees, beneficiaries, and other individuals and entities associated with DHS and Departmental programs and activities. These investigations can result in criminal prosecutions, fines, civil monetary penalties, and administrative sanctions. Additionally, OIG's Office of Investigations oversees and monitors the investigative activity of the DHS Components' various internal affairs offices.

As part of OIG's investigative responsibilities, during the course of the investigation and evidence-gathering, OIG's Office of Investigations may search and extract information from digital and multimedia devices, which may include: mobile phones, laptops, digital cameras, thumb drives, and other devices capable of storing electronic information. Pursuant to the nature of and allegations made in the underlying investigation, the electronically stored information (ESI) maintained on these electronic devices may be classified. Because of this, the OIG's Office of Investigations' Digital Forensics and Analysis Unit (DFAU) will operate a stand-alone Classified Digital Forensic Workstation (CDFW) to process the electronically stored information on the digital and multimedia evidence devices referenced above for examination. The CDFW will be used for digital forensic acquisition (creating an image or duplicate of the original data) and/or

[1] U.S.C. App. 3.

extraction of source media. The data on the workstation will be processed using authorized specialized digital forensic software or applications for review and analysis. Following the processing and analysis of the electronically stored information, the information will be transferred and stored on the highest-classification level information system, or, when classified information is not located, the information will be appropriately sanitized, redacted, and down-graded to an unclassified level. The unclassified data will be stored within OIG's Office of Investigations' Enforcement Data System (EDS) which is the official OIG case management system for OIG's investigations.[2] The OIG Office of Investigations and the Office of Counsel, including the Whistleblower Protection Division, uses the Enforcement Data System to manage information relating to complaints and investigations of alleged criminal, civil, or administrative violations by DHS employees, contractors, grantees, beneficiaries, whistleblowers, and other individuals and entities associated with DHS. The Enforcement Data System allows investigators and counsel to manage investigations initiated from those complaints to facilitate the tracking of resources used in investigative activities.

The information collected from the digital and multimedia devices is stored for the entirety of the investigation and any subsequent actions on the CDFW and/or the Enforcement Data System, depending on classification level. Upon conclusion and determination that the information is no longer needed, it is securely wiped or destroyed in accordance with the appropriate retention schedule and DHS device sanitization guidelines.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Inspector General Act of 1978, as amended, and the Homeland Security Act of 2002[3] permit the DHS OIG to collect information necessary for the OIG to perform audits, inspections, investigations, and legal analysis on programs and operations within the Department. DHS Management Directive 0810.1[4] assigns the OIG the responsibility to "receive and investigate complaints or information from employees, contractors, and other individuals concerning the possible existence of criminal or other misconduct constituting a violation of law…." This Directive also provides instructions on the roles and responsibilities of DHS Organizational Elements and DHS employees pertaining to the collection of data provided to the OIG. Additionally, OIG's Office of Investigations obtains authority through consent, search warrants,

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF INSPECTOR GENERAL, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT DATA SYSTEM, DHS/OIG/PIA-001 OIG (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-office-inspector-general-oig.
[3] 6 U.S.C. § 101.
[4] Department of Homeland Security Management Directive System, MD Number 0810.1 (June 10, 2004), https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_0810_1_the_office_of_inspector_general.pdf.

court orders, subpoenas, and other legal procedures to obtain evidence in its investigations, which may require analysis and review on the CDFW. When authorized by a search warrant, the CDFW's digital forensic application or software tools may be used to overcome security and encryption challenges on a locked electronic device.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The OIG Investigative Records System of Records Notice (SORN) covers the information and records the OIG processes during its audits, inspections, and investigations and incorporates it into its reports.[5] This System of Records Notice also covers the collection of information from other government agencies, commercial sources, and publicly available sources.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

CDFW is going through the security Certification and Accreditation process to obtain an Authority to Operate (ATO) and will comply with all requirements under DHS Management Directive 4300A.[6] The CDFW contains industry-standard digital forensics software tools used to image, process, and analyze data obtained during criminal investigations. The system, including these tools, has had vulnerability testing performed in a manner with DHS information security policy prior to deployment. The Authority to Operate will be obtained when all accreditation processes are completed, including this Privacy Impact Assessment.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Retention of CDFW records will be governed by N1-563-07-5[7], Item 1, which states all investigative case files, except for those determined to be unusually significant, are temporary and are to be destroyed twenty (20) years after completion of the investigation and all subsequent actions. Destruction of the data will consist of deletion from the CDFW workstation, destruction of any optical media, and secure wiping of any USB thumb drives where data may be stored. Data within CDFW related to cases determined to be unusually significant will be permanently retained in accordance with Items 2 and 5 of N1-563-07-5.

---

[5] *See* DHS/OIG-002 Investigative Records System of Records Notice, 86 Fed. Reg. 58292 (October 21, 2021).
[6] DHS 4300A Sensitive System Handbook is a series of information security policies, which are the official documents that create and publish Departmental security standards in accordance with DHS Management Directive 140-01, Information Technology System Security. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS 4300A SENSITIVE SYSTEMS HANDBOOK, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.
[7] *See* DHS OIG NARA Retention Schedule #N1-563-07-5, https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-07-005_sf115.pdf.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected as part of this system is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The information stored within CDFW is collected during OIG investigations and obtained through the imaging of digital devices seized during an active investigation for examination. The imaging information is not manually entered into the workstation. Depending on the file size of the electronically stored information, the information may either be transferred directly onto a CD or USB which will then be connected to the workstation, or the physical device that is obtained during the investigation (such as a personal phone) will be directly connected to the CDFW. Information collected from the digital device may include:

- The names and personally identifiable information of subjects, victims, witnesses, or other individuals associated with the investigation;
- Images, emails, text messages, or other electronic communications that may include personally identifiable information related to the subjects, victims, witnesses, or other individuals associated with the investigation;
- Bank records related to the subjects, victims, witnesses, or other individuals associated with the investigation;
- Business records related to the subjects, victims, witnesses, or other individuals associated with the investigation; and
- Any other personal information that is located on the digital device image.

2.2 What are the sources of the information and how is the information collected for the project?

The CDFW collects and stores data obtained from digital devices (e.g., cell phones, tablets, laptops) obtained during the course of the investigation. The data is collected using digital forensics tools that create a logical or physical copy of the data on them in the form of an image file or files. Depending on the file size of the electronically stored information, the information

may either be transferred directly onto an optical disk or USB drive, which will then be connected to the workstation, or the physical device that is obtained during the investigation (such as a personal phone) will be directly connected to the CDFW.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

CDFW has no direct connections to nor explicitly collect any information obtained from commercial or publicly available sources. Devices imaged pursuant to appropriate authorities may have user-downloaded content from external sources, such as social media. However, no information is directly obtained from any commercial or public source by DHS OIG on the CDFW.

2.4 Discuss how accuracy of the data is ensured.

Any data provided and obtained during the investigation will be verified for accuracy as part of the investigation through generally accepted digital forensics practices (e.g., hash values,[8] chain of custody documents), with digital images of the devices involved serving as an official record. Upon seizure of a digital device, either extraction of relevant information is made from the device using the digital forensic applications CDFW uses, or an image of the device's entire contents is produced, which creates a duplicate or mirror copy on the CDFW that is used for analysis. Image files copied to CDFW are reviewed for authenticity and integrity as part of the acquisition process.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that more information than necessary is collected.

Mitigation: This risk is partially mitigated. Collection of information by OIG is tailored to the scope of the investigation. Due to the nature of investigative efforts, however, devices are generally fully imaged, and searches are conducted on those images following their acquisition. This process, out of necessity, frequently involves the acquisition of unrelated information stored on these devices. While forensic search and review protocols are targeted toward responsive information, requirements to maintain best-evidence copies of records for discovery purposes necessitates this information be retained throughout the legal proceedings.

Although it may not be possible to know in advance what information may turn out to be relevant and necessary, to partially mitigate this risk, OIG's collection of information relies on and is governed by the oversight of the courts through existing law enforcement and legal procedures,

[8] Hash values are mathematical signatures that map extensive data to fixed-size representations for comparison and change detection purposes.

including consent by the individual, search warrants, court orders, and subpoenas (e.g., search warrants, for example, require specificity in both the items to be seized/imaged and analysis (searches) that may be conducted).

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

OIG's Office of Investigations investigates allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, grantees, and programs. As part of an active investigation, digital devices may be seized and imaged, or records/device images may be obtained through other legal procedures. That information may be used as evidence to support an allegation of wrongdoing. This information is transferred, analyzed, and stored in the CDFW.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

The CDFW does not perform any such analyses.

3.3 Are there other components with assigned roles and responsibilities within the system?

There are no other components with access to the CDFW.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information may be accessed without a valid need-to-know.

Mitigation: The risk is mitigated. The CDFW is maintained in a sensitive compartmented information facility (SCIF), limiting physical access. Further, a very limited number of personnel have logical access to this system. All personnel accessing the data are required to have the proper security clearance in place as well as an established need-to-know. Moreover, to ensure the required steps are followed, personnel who have the required need-to-know and proper security clearance are required to complete Cybersecurity Awareness Training, Privacy Training, Clearance Holders Annual Refresher Training, SCI Annual Refresher Training, SCI IT Security Awareness Training, and the Federal Acquisition Institute (FAI) Cornerstone OnDemand (CSOD) training. CDFW users are additionally required to meet the training requirements for digital forensics, including the proper handling and management of digital evidence, consistent with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Digital

Forensics.[9]

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

DHS provides notice to the public through this Privacy Impact Assessment and the OIG Investigative Records System of Records Notice. When Special Agents interact with individuals in connection with an investigation, the electronic devices tied to the subject may be collected. For consensual acquisitions, the individual provides written, informed consent specific to the allegation by signing an OIG consent form. For acquisition through legal procedures, notice is provided as appropriate (e.g., a copy of a warrant). For government-furnished equipment (GFE), as part of DHS Baseline configurations, any workstations collected that are government-furnished equipment were already required to have a "default" banner that should reference consent to be monitored. This may not appear on government furnished equipment phones but are integrated as part of the DHS Rules Of Behavior (RoB) and possibly within each Component's Rules of Behavior, such as that of OIG's Rules of Behavior.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

For consensually acquired device images and content, individuals can opt out of collection or limit the collection to specific items. However, there is generally no ability to opt out for court ordered acquisitions,, though individuals retain the right to contest in court any such acquisition as permitted by law. For government-furnished equipment, individuals consent to monitoring at the time of usage.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There may be isolated cases where notice is not provided to the subject of the investigation (e.g., with a no-notice warrant or acquisition of business records from a DHS system), such as when data is obtained from a cell phone.

Mitigation: This risk is not mitigated. However, the exceptions to this notice requirement are expected to be minimal and limited. Although the lack of notice poses a privacy risk, due to the nature of OIG investigations, providing notice in these limited situations may potentially jeopardize the integrity of an investigation and present a risk of destruction of evidence.

Privacy Risk: There is a risk that OIG will obtain personally identifiable information

[9] *See* https://www.ignet.gov/content/quality-standards.

pertaining to unrelated third parties when such information is maintained on the subject of the investigation's digital device.

Mitigation: This risk is not mitigated. Given the purpose of the collection, it would be impossible for OIG to identify and know all information maintained on a subject's digital device (e.g., phone) prior to extraction and digital forensic processing and analysis. Although the lack of notice poses a privacy risk, especially to the third parties who may not be under investigation, OIG only uses information extracted and analyzed that is relevant to the underlying case during the investigative process. The information that is not relevant and pertains to the unrelated parties is properly maintained in either a classified information system or in the Enforcement Data System, with appropriate security and access controls in place, and is destroyed upon completion of the investigation and any subsequent actions according to NARA-approved records retention schedules.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

Information is retained for the purpose of resolving allegations of wrongdoing and to fully identify all those related to a criminal investigation. Retention of data within CDFW will be governed by the NARA-approved records schedule, N1-563-075, Item 1, which states all investigative case files, except for those determined to be unusually significant, are temporary and are to be destroyed twenty (20) years after completion of the investigation and all subsequent actions. Additionally, individual prosecutorial guidance will guide temporary data retention for specific cases. The destruction of the data will consist of deleting it from the CDFW workstation or external data devices. Data within CDFW related to cases determined to be unusually significant will be retained permanently in accordance with N1-563-07-5, Item 2.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information maintained in CDFW will be maintained longer than is necessary, especially that information deemed unusually significant and thus maintained permanently.

Mitigation: This risk is mitigated. The CDFW is not intended to store data long-term, and any archival case files will be offloaded onto other storage media, with entries made into the OIG's Office of Investigations' Enforcement Data System indicating the type and location of the data. As part of automated case-closing procedures within the Enforcement Data System, confirmation of the deletion of all temporary evidence must be indicated and approved. Additionally, for long-term data retention, the digital archiving procedures in the case management system include obtaining any externally stored information for transmission per NARA procedures.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

OIG may share corresponding investigative information on a Classified level with individuals from other law enforcement agencies with the appropriate Classification level and a verified need-to-know, as well as Congress on an as needed-basis and with the appropriate Classification level, pursuant to OIG's authorities and responsibilities. Unclassified information pertaining to an investigation may also be provided to prosecutors, defense attorneys, the trial court, and the Merit Systems Protection Board (MSPB) for administrative cases pertaining to employee misconduct. Sharing of any classified information for court purposes will comply with the Classified Information Procedures Action.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The sharing of data maintained on the CDFW is authorized under the OIG Investigative Records System of Records Notice. As an example, the information shared is done so in accordance with the following routine uses:

A. The Department of Justice, including Offices of the U.S. Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation; and

G. Appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

6.3 Does the project place limitations on re-dissemination?

DHS OIG does place limitations on the re-dissemination of data in CDFW. CDFW consists of data that is both Classified and Law Enforcement Sensitive information. When sharing information with another DHS Component or externally, as authorized by the OIG Investigative Records System of Records Notice and other authorities, it is performed on a need-to-know basis, and only the information that is required is shared. Notice is routinely provided by DHS OIG on reports containing the shared data that the report remains the property of the OIG, and no secondary distribution may be made, in whole or in part, outside DHS, without prior authorization by the

OIG. The sharing of data externally is memorialized as an action in the Enforcement Data System, which includes the specific information shared and the date of the sharing. Data being provided externally is redacted and sent as Unclassified, when possible, as is the preferable approach, by leveraging an application from DHS called Swift with a reliable human reviewer to downgrade data from Top Secret, Secret, or Confidential to Unclassified. Any declassification of data must be approved by an approved Classification Authority and in accordance with declassification guidelines. If data cannot be unclassified, for any disclosures to external parties, the data must be provided from one classified network to another, as long as there is a need-to-know and a DHS security officer has confirmed the recipient to possess the appropriate clearance to view the information.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The CDFW resides in the DHS SCIF. OIG must follow all DHS SCIF compliance rules, which includes how data located within is shared. Sharing of records is tracked in the OIG's Office of Investigations case management system, the Enforcement Data System, through case notes and via a sign in/out log within the SCIF for removable media. In addition, devices that are connected to the CDFW are logged internally within the workstation's System Logs which includes USB drives and optical disks. Once devices and files leave the DHS SCIF, tracking of data then falls outside of both the CDFW and DHS SCIF boundaries. Classified data physically leaving the SCIF requires proper standard markings, cover sheets or envelopes as dictated within the annual trainings pertaining to clearance holders, and will be performed in accordance with DHS regulations governing the transportation of classified information.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information from CDFW could be shared inappropriately.

Mitigation: The risk is mitigated. Access to data on the CDFW is authorized only to those OIG employees with a need-to-know and a proper security clearance in place. If data that is maintained on the CDFW is shared externally with another agency or with another DHS Component, the information will need to either be declassified, be shared from one classified environment to another classified environment, or the appropriate individual will go through the proper SCIF protocols. Only individuals with a valid need-to-know will be provided access to data on the CDFW, regardless of classification level.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Due to the nature of the information maintained on the CDFW, certain records may be exempt from requests for access by covered individuals to the extent permitted by the Privacy Act and the OIG Investigative Records System of Records Notice. U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act (JRA) may still file a Privacy Act request to access their information, and, depending on a determination made by DHS OIG, those records may be released.

Notwithstanding, all individuals seeking access to their records may submit a Privacy Act request at https://www.oig.dhs.gov/foia. Requests can also be made by email, telephone, or mail:

OIG Office of Counsel
245 Murray Lane SW Mail Stop - 0305
Washington, D.C. 20528-0305
Phone: 202-981-6100
Fax: 202-245-5217
FOIA.OIG@OIG.DHS.GOV

All requests must conform to the Privacy Act regulations set forth in federal regulations and are evaluated to ensure that the release of information is lawful, will not impede an investigation, and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

In addition, to the extent OIG maintains information or data that another DHS Component or federal agency provided as part of an investigation, that information is maintained within the OIG Investigative Records System of Records in a secured and protected manner in accordance with proper protocols. If a requestor makes a request , and information and/or data that is another Component's or agency's information is located as part of the search for the responsive material, OIG will either consult with the appropriate Component or agency prior to releasing the information or will refer the information to the Component or agency for direct response and release to the requestor.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The procedures for correcting inaccurate or erroneous information are similar to the redress procedures in Section 7.1 above. Individuals may not be able to correct the record for information within CDFW because it may be part of a confidential investigation, and releasing an individual's

records or allowing them to correct those records may impede the investigation. However, covered individuals may submit a Privacy Act Amendment request as outlined above.

7.3 How does the project notify individuals about the procedures for correcting their information?

This Privacy Impact Assessment and the OIG Investigative Records System of Records Notice provides notice to individuals regarding how to access and correct their information. Requests to amend or correct information about themselves will be handled under the Privacy Act of 1974, 5 U.S.C. § 552a(d).

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not know what procedures exist for collecting or correcting information.

Mitigation: This risk is mitigated. This Privacy Impact Assessment and the OIG Investigative Records System of Records Notice provide information on requesting access and amendment to information maintained within the CDFW. Moreover, individuals have the ability to inquire about the information the federal government maintains on them. They may submit a FOIA or Privacy Act request, as applicable, to DHS at any time. If the individual's request to obtain records is denied in full or in part, they have the right to appeal their denial to the FOIA/Privacy Act Appeals Unit. Individuals also have the opportunity to seek dispute resolution services through the FOIA Public Liaison, whose contact information can be located on the DHS OIG website.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

CDFW requires the proper security clearance and access to the SCIF where the CDFW is physically located. Users can only access the CDFW in person as the system is a stand-alone system with no direct connection to any network. The CDFW will log users who sign into the device and log external devices that connect to the system. Logs are reviewed on a quarterly basis by OIG's Reliable Human Reviewers (RHR) or delegated personnel. Additionally, the OIG security team will perform the following audit techniques within the CDFW prior to deployment:

- Independent Verification and Validation (IV&V);
- Risk Assessments;
- Vulnerability Scanning; and
- Third-party audits.

The OIG is also subject to inspection by the Committee on Inspector General Integrity and Efficiency (CIGIE).[10] These inspections may review the OIG's use of how the classification of data and sensitivity of data are being handled to determine if the system is being used in accordance with its stated purpose.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OIG employees are required to take annual security awareness and role-based training. All DHS OIG employees, including contractors, are also required to participate in mandatory annual privacy training. Furthermore, all DHS personnel accessing data maintained on the CDFW are required to have the proper security clearance in place, a valid need-to-know, and are to follow the steps that have been outlined in the required Clearance Holders Annual Refresher Training, SCI Annual Refresher Training, SCI IT Security Awareness Training, and the Federal Acquisition Institute (FAI) Cornerstone OnDemand (CSOD) training. CDFW users are also required to meet digital forensics training requirements, including the proper handling and management of digital evidence, consistent with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Digital Forensics.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to investigative information is determined by an individual need-to-know for each piece of imaged content. The CDFW is only accessible in person as it is a standalone workstation with no connection to any network, and therefore, access to remote desktop capabilities does not exist. Physical access to the CDFW is controlled as listed in Section 8.1 above. In addition, access to the CDFW consists of a UserID and password associated with each individual account created by the system administrator. Initial access to the system is configured to require the user to change their password immediately. Moreover, access will be further controlled using defined roles and restrictions to the system and for each piece of imaged content as necessary.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All project reviews, approved information sharing, Memorandum of Understanding

[10] CIGIE is an independent entity established within the Executive Branch to address integrity, economy, and effectiveness issues that transcend individual government agencies and aid in the establishment of a professional, well-trained, and highly skilled workforce in the Offices of Inspectors General. *See* https://www.ignet.gov/.

(MOU), Memorandum of Agreement (MOA), and other new data information uses for CDFW must comply with DHS Sensitive Systems Handbook and Policy Directive 4300A. All appropriate documentation and requirements must be approved by all authorizing officials of each system such as:

- System Owner (SO);
- Chief System Security Officer (CISO);
- Information System Security Manager (ISSM);
- Information System Security Officer (ISSO); and
- Program Manager (PM)

Contact Official

Chad Steel
Special Agent in Charge
Office of Investigations
Office of Inspector General
U.S. Department of Homeland Security

Responsible Official

Darcia Rufus
Acting Division Chief-Information Law and Disclosure
Office of Inspector General
U.S. Department of Homeland Security

Approval Signature

Original, signed version on file with the DHS Privacy Office.

_____

Deborah T. Fleischaker
Chief Privacy Officer (A)
U.S. Department of Homeland Security
privacy@hq.dhs.gov