United States Department of Justice (DOJ)

Office of Privacy and Civil Liberties (OPCL)

Privacy Impact Assessment
for the
USA Relativity D-GC

Issued by:
Kevin Krebs
Senior Component Official for Privacy

Approved by: Christina Baptista
Senior Counsel, Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: December 5, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

USA Relativity D-GC is the EOUSA instance of the Deloitte Evidence Management System. The purpose of USA Relativity D-GC is to provide a secure, web-enabled application that stores, produces, and processes electronic evidence. The application is used by US Attorney's Office (USAO) personnel nationwide to manage litigation needs including processing, importing, exporting, and producing evidentiary data. The application allows end-users to effectively review, search, analyze and redact evidentiary data in support of litigation cases.

EOUSA has prepared a Privacy Impact Assessment for USA Relativity D-GC because this system collects, maintains, and disseminates information in identifiable form about individuals for the purposes of discovery during the course of litigation (for more detail, see data types checked and outlined in the table in Section 3.1).

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

USA Relativity D-GC provides a secure, web-enabled document review and management platform utilized for e-discovery, investigations, and litigation in criminal and civil matters. USA Relativity D-GC supports the analysis, review, and production of electronic discovery. The system has the ability to handle large, complex e-discovery projects and provides imaged and native file review, Unicode and foreign language support, and full-text and concept-based searching.

The information in USA Relativity D-GC is obtained from federal records, opposing parties and third parties. Collected information is imported to USA Relativity D-GC in a digital format for a particular investigation or litigation, where it is cataloged, indexed, processed, and archived. The USAOs can securely view, process, analyze and report upon information and data related to a case using the information within USA Relativity D-GC.

Access is provided to internal DOJ users, other federal government users, state or local government users, and certain members of the public that comply with the established rules of the Network Account Security Management (NASM) United States Attorneys' Procedures (USAP). An example of such a member of public would be an expert witness under contract with DOJ who may need to review documents related to a case. Access for the receipt of information and data may be provided to commercial data sources, such as credit reporting agencies, closed-circuit television (CCTV) operators, mobile phone networks, social media platforms, and credit card companies, pursuant to established agreements with the USAO. The requested information may be transferred to USA Relativity D-GC by direct log in access by the external entity or through the transfer of physical media.

Access to USA Relativity D-GC data is strictly controlled, with users having access only to

that data for which they are authorized. All such access must comply with DOJ requirements and must support EOUSA/USAO investigation and litigation needs. The USA Relativity D-GC system manages user authorizations and access to information, including for views, searches, and sorting activities to analyze documents and determine which are relevant to a case.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	• 5 USC § 301 • 44 USC § 3301 (for the purposes of implementing provisions of 5 U.S.C. 552 and 5 U.S.C. 552a) • 28 USC Ch. 35 • Federal Information Security Modernization Act of 2014, 44 USC § 101 note
Executive Order	
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, and D	Full Names of individuals mentioned in case files may be included.
Date of birth or age	X	A, B, C, and D	Date of birth of individuals mentioned in case files may be included.
Place of birth	X	A, B, C, and D	Place of birth of individuals mentioned in case files may be included.
Sex	X	A, B, C, and D	Sex of individuals mentioned in case files may be included.
Race, ethnicity, or citizenship	X	A, B, C, and D	Race, ethnicity or citizenship of individuals mentioned in case files may be included.
Religion	X	A, B, C, and D	Religion of individuals mentioned in case files may be included.
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	Social Security Number (full, last 4 digits or otherwise truncated) of individuals mentioned in case files may be included.
Tax Identification Number (TIN)	X	A, B, C, and D	Tax Identification Number (TIN) of individuals mentioned in case files may be included.
Driver's license	X	A, B, C, and D	Driver's licenses of individuals mentioned in case files may be included.
Alien registration number	X	A, B, C, and D	Alien registration numbers of individuals mentioned in case files may be included.
Passport number	X	A, B, C, and D	Passport numbers of individuals mentioned in case files may be included.
Mother's maiden name	X	A, B, C, and D	Mother's maiden name of individuals mentioned in case files may be included.
Vehicle identifiers	X	A, B, C, and D	VINs, and license plate numbers mentioned in case files may be included.
Personal mailing address	X	A, B, C, and D	Personal mailing addresses of individuals mentioned in case files may be included.
Personal e-mail address	X	A, B, C, and D	Personal e-mail addresses of individuals mentioned in case files may be included.
Personal phone number	X	A, B, C, and D	Personal phone numbers o of individuals mentioned in case files may be included.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Medical records number	X	A, B, C, and D	Medical records numbers of individuals mentioned in case files may be included.
Medical notes or other medical or health information	X	A, B, C, and D	Medical notes or other medical or health information mentioned in case files may be included.
Financial account information	X	A, B, C, and D	Financial account information of individuals mentioned in case files may be included.
Applicant information	X	A, B, C, and D	Applicant information of individuals mentioned in case files may be included.
Education records	X	A, B, C, and D	Education records of individuals mentioned in case files may be included.
Military status or other information	X	A, B, C, and D	Military status or other information of individuals mentioned in case files may be included.
Employment status, history, or similar information	X	A, B, C, and D	Employment status, history, or similar information of individuals mentioned in case files may be included.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, and D	Performance improvement plan, warnings or reprimands of individuals mentioned in case files may be included.
Certificates	X	A, B, C, and D	Certificates mentioned in case files may be included.
Legal documents	X	A, B, C, and D	Legal documents mentioned in case files may be included.
Device identifiers, e.g., mobile devices	X	A, B, C, and D	Device identifiers mentioned in case files may be included.
Web uniform resource locator(s)	X	A, B, C, and D	Web uniform resource locator(s) mentioned in case files may be included.
Foreign activities	X	A, B, C, and D	Foreign activities of individuals mentioned in case files may be included.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	Criminal records information of individuals mentioned in case files may be included.
Juvenile criminal records information	X	A, B, C, and D	Juvenile criminal records information of individuals mentioned in case files may be included.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, and D	Civil law enforcement information mentioned in case files may be included.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C, and D	Whistleblower information mentioned in case files may be included.
Grand jury information	X	A, B, C, and D	Grand jury information mentioned in case files may be included.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, and D	Information concerning witnesses to criminal matters mentioned in case files may be included.
Procurement/contracting records	X	A, B, C, and D	Procurement/contracting records mentioned in case files may be included.
Proprietary or business information	X	A, B, C, and D	Proprietary or business information mentioned in case files may be included.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, and D	Location information mentioned in case files may be included.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, and D	Photographs or photographic identifiers of individuals mentioned in case files may be included.
- **Video containing biometric data**	X	A, B, C, and D	Video containing biometric data of individuals mentioned in case files may be included.
- **Fingerprints**	X	A, B, C, and D	Fingerprints of individuals mentioned in case files may be included.
- **Palm prints**	X	A, B, C, and D	Palm prints of individuals mentioned in case files may be included.
- **Iris image**	X	A, B, C, and D	Iris images of individuals mentioned in case files may be included.
- **Dental profile**	X	A, B, C, and D	Dental profiles of individuals mentioned in case files may be included.
- **Voice recording/signatures**	X	A, B, C, and D	Voice recordings/signatures of individuals mentioned in case files may be included.
- **Scars, marks, tattoos**	X	A, B, C, and D	Scars, marks, tattoos of individuals mentioned in case files may be included.
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C, and D	Vascular scans of individuals mentioned in case files may be included.
- **DNA profiles**	X	A, B, C, and D	DNA profiles of individuals mentioned in case files may be included.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Other (specify)**	X	A, B, C, and D	Because of the varied nature of the records subject to disclosure, other types of PII not listed above may be collected, maintained or disseminated.
System admin/audit data:			
- **User ID**	X	A, B, C, and D	User ID of DOJ users, corporate counsels, litigators and government attorneys.
- **User passwords/codes**	X	A, B, C, and D	User passwords/codes of DOJ users, corporate counsels, litigators and government attorneys.
- **IP address**	X	A, B, C, and D	IP address of DOJ users, corporate counsels, litigators and government attorneys.
- **Date/time of access**	X	A, B, C, and D	Date/time of access of DOJ users, corporate counsels, litigators and government attorneys.
- **Queries run**	X	A, B, C, and D	Queries run of DOJ users, corporate counsels, litigators and government attorneys.
- **Contents of files**	X	A, B, C, and D	Content of files accessed/reviewed of DOJ users, corporate counsels, litigators and government attorneys.
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	Because of the varied nature of the records in case files or subject to discovery in litigation, other types of PII not listed above may be collected, maintained or disseminated.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	
Phone		Email			
Other (specify): The information in USA Relativity D-GC is not collected directly from individuals into the system, but may originally have been collected from individuals.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X

Government sources:					
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): Foreign sources of information include information sharing agreements that further the mission of DOJ, such as: *Agreement Between the Government of the United States and the Government of Canada Regarding the Application of their Competition and Deceptive Marketing Practices*, and *U.S.-Canada Cooperation Agreement; Migrant Protections Protocol*.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers	X				
Other (specify): Commercial data sources may include credit reporting agencies, closed-circuit television (CCTV) operators, mobile phone networks, social media platforms, and credit card companies. USAOs establish agreements, such as MOUs, with these entities to govern the transfer of information. The requested information may be transferred to USA Relativity D-GC by direct log in access by the external entity or through the transfer of physical media.					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X		X	Deloitte personnel will upload case data to USA Relativity D-GC via web browser. All other USAO personnel involved in a potential case can only review the information via web browser.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
DOJ Components	X		X	Deloitte personnel will upload case data to USA Relativity D-GC via web browser. Other members of a federal case team can only review the information via web browser.
Federal entities	X		X	Deloitte personnel will upload case data to USA Relativity D-GC via web browser. Other members of a federal case team can only review the information via web browser.
State, local, tribal gov't entities	X		X	Deloitte personnel will upload case data to USA Relativity D-GC via web browser. Other members of a federal case team can only review the information via web browser.
Public	X		X	Deloitte personnel will upload case data to USA Relativity D-GC via web browser. Other members of a federal case team can only review the information via web browser.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X		X	Deloitte personnel will upload case data to USA Relativity D-GC via web browser. Other members of a federal case team who are involved in a potential case can only review the information via web browser. On rare occasions (I.E., by court order), adverse external users (Non-federal person who represents parties in opposition to the government (I.E., opposing counsel) as defined by the Network Account Security Management (NASM) No. 3-16-200-003) may review case data in

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
				USA Relativity D-GC via web browser.
Private sector	X		X	Deloitte personnel will upload case data to USA Relativity D-GC via web browser. Other members of a federal case team who are involved in a potential case can only review the information via web browser.
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

The information contained in USA Relativity D-GC will not be released to the public for "Open Data" purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

The information in this system is not specifically collected from individuals. The information is part of case files required for investigations and litigation. System of Records Notices (SORNs) covering civil and criminal case files have been published in the Federal Register that provide a generalized notice to the public:

DOJ/USA-005, "Civil Case Files," last published in full at 53 Fed. Reg. 1864 (Jan. 22, 1988), available at: https://www.justice.gov/opcl/docs/usa-005-53fr1864.pdf.

DOJ/USA-007, "Criminal Case Files," last published in full at 53 Fed. Reg. 1864 (Jan. 22, 1988), available at: https://www.justice.gov/opcl/docs/usa-007-53fr1864.pdf.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the

collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

The information in this system is not collected directly from individuals, but is collected from case files required for investigations and litigation. Therefore, individuals will not have the opportunity to opt out of the collection into, use of, or dissemination of their information from USA Relativity D-GC.

Information on Federal case team members will be captured through USAAuth, which is a mechanism for trusted single sign-on for internal and external users to United States Attorneys applications, and is required for auditing purposes. Federal case team members will not have the opportunity to opt out of providing this information.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

The information in this system is not collected directly from individuals, but is collected from case files required for investigations and litigation. Therefore, individuals will not have the access to the information in USA Relativity D-GC or the opportunity to opt out of the collection into, use of, or dissemination of their information from USA Relativity.

Information on Federal case team members will be captured through USAAuth, which is a mechanism for trusted single sign-on for internal and external users to United States Attorneys applications, and is required for auditing purposes. Federal case team members will not have the opportunity to opt out of providing this information.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** USA Relativity D-GC was authorized on 9/23/24 and expires on 9/23/27. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide**

	a link to the applicable POAM documentation: POA&M #40761 has been created to track the creation of the USA Relativity D-GC PIA.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** USA Relativity D-GC has an overall FISMA security categorization of moderate based on the types of information it contains, and consequently, EOUSA has implemented FedRAMP moderate baseline controls for the system.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The implemented FedRAMP moderate baseline controls undergo control assessments on an annual basis to ensure they are properly implemented. Assessment includes vulnerability testing, compliance monitoring, and control evaluation.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** USA Relativity D-GC audits and creates logs for all activities within USA Relativity D-GC. All account auditing is conducted by the EVIDENCE MANAGEMENT SYSTEM (EMS)team and is not in scope for EOUSA. All account reviews are conducted by the USA RelativityD-GC System Owner or Account Manager quarterly for service accounts and annually for Client User accounts.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** Both general information security and privacy training and training specific to the system is conducted for authorized users within the Department.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

Access controls are implemented to ensure only authorized users have access to the information collected, in addition to only being granted the privileges necessary to accomplish their job duties. Additionally, there are safeguards implemented to ensure that unauthorized access to the system is not granted and the risk of unauthorized disclosure of the information within the system is minimized.

To obtain an account with USA Relativity D-GC, the USA Relativity D-GC Client User must send an email to the USA Relativity D-GC account manager to request an account to be created. Once the request is approved by the USA Relativity D-GC account manager, the account manager will forward the request to the EMS team for account creation. USA Relativity D-GC audits and creates logs for all activities within USA Relativity D-GC. All account auditing is conducted by the EMS team and not in scope for EOUSA. All account reviews are conducted by the USA Relativity D-GC System Owner or Account Manager quarterly for service accounts and annually for Client User accounts. An open session within the information system will also be subject to session termination in cases of inactivity.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

The data in the USArelativityD-GC system is maintained for as long as needed by the authorized DOJ users, corporate counsels, litigators and government attorneys and are subject to the respective retention periods that govern them, e.g., NARA General Records Schedules, agency SF-115s, and any applicable SORNs published under the Privacy Act of 1974, 5 U.S.C. §552a (see https://www.justice.gov/opcl/doj-systems-records).

Procedures have been developed to ensure that electronic copies are not, in practice, retained beyond the retention period established for the original records and will be disposed of in accordance with DOJ Network Account Records Management USAP No. 3-13.300.004 (https://usanetsp.usa.doj.gov/usaps/SitePages/All%20Active%20USAP.aspx)

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

___X__ No. _____ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

- DOJ/USA-005, "Civil Case Files," last published in full at 53 Fed. Reg. 1864 (Jan. 22, 1988), available at: https://www.justice.gov/opcl/docs/usa-005-53fr1864.pdf.

- DOJ/USA-007, "Criminal Case Files," last published in full at 53 Fed. Reg. 1864 (Jan. 22, 1988), available at: https://www.justice.gov/opcl/docs/usa-007-53fr1864.pdf.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

In any circumstance, the disclosure or sharing of information increases risks to privacy. In this case, EOUSA takes a number of measures to reduce the risk of unauthorized disclosure and potential data breach. All EOUSA component systems are subject to consistent assessment and authorization processes that ensure that security controls are in place to protect the confidentiality, integrity, and availability of all information and the systems that house that information.

Specifically:

- The principle of least privilege is enforced to ensure those who have access are only granted the minimum access required based on job duties;
- All EOUSA component staff require mandatory security awareness and role-based training on an annual basis;
- All users of the system must acknowledge Rules of Behavior before receiving an account to access the system and review case files;
- Account access for users is managed by EMS team and granted on an as-needed basis, with the principle of least privilege enforced to restrict what the user can access; and
- User actions are audited by the EMS team to identify any unauthorized user actions, such as data exfiltration or modification/deletion.

Additionally, all security controls were tested prior to system authorization and implementation. Other security control families that are tested and implemented as safeguards include: Auditing, Contingency Planning, Incident Response, Media Protection, Physical Protection, Risk Assessment, and System and Information Integrity. These control families are reviewed by the ISSO and independent assessors to ensure all controls are implemented accurately and the system is operating as intended.