

United States Department of Justice (DOJ)  
Office of Privacy and Civil Liberties (OPCL)



**Privacy Impact Assessment**  
for the  
USA Litigation Management Application (USALMA-c)

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: June 6, 2025

*(May 2022 DOJ PIA Template)*

## **Section 1: Executive Summary**

USA Litigation Management Application (USALMA-c) is the EOUSA instance of the Everlaw SaaS solution (“Everlaw”). EOUSA has prepared a Privacy Impact Assessment for USALMA-c 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).

Everlaw is a cloud-based platform used by the United States Attorneys’ Offices (USAOs) for organizing, reviewing, managing, and producing information collected during the discovery phase of litigation.

## **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.*

The Everlaw Platform is a Government Software as a Service (SaaS) product and can be deployed as a Government Only Community or a Virtual Private Cloud (VPC). The Everlaw Platform is a single web application that is accessed via the internet. The system components of the Everlaw Platform are hosted in a VPC in the AWS US East 1 region.

The USAO Litigation Support Specialists upload case data to the Everlaw Platform via web browser. The information in this system is not collected directly from individuals. Rather, it is information gathered from a variety of sources, including other federal, state and local partners, foreign government partners, opposing counsel, pro se litigants, investigators, and members of the public. The information is reviewed and used by USAOs to build and support their cases in a court of law. The USAOs use USALMA-c to securely view, process, analyze and report upon information and data related 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.)*

<b>Authority</b>	<b>Citation/Reference</b>
Statute	<ul style="list-style-type: none"><li>• 5 U.S.C. § 301</li><li>• 44 U.S.C. § 3301 (for the purposes of implementing provisions of 5 U.S.C. 552 and 5 U.S.C. 552a)</li><li>• 28 U.S.C. Ch. 35</li><li>• Federal Information Security Modernization Act of 2014, 44 U.S.C. § 101 note</li></ul>
Executive Order	<ul style="list-style-type: none"><li>• Homeland Security Presidential Directive 12</li></ul>
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
<i>Example: Personal email address</i>	X	B, C and D	<i>Email addresses of members of the public (US and non-USPERs)</i>
<b>Name</b>	X	A, B, C, and D	Full Names of individuals mentioned in case files may be included.
<b>Date of birth or age</b>	X	A, B, C, and D	Date of birth of individuals mentioned in case files may be included.
<b>Place of birth</b>	X	A, B, C, and D	Place of birth of individuals mentioned in case files may be included.
<b>Sex</b>	X	A, B, C, and D	Sex of individuals mentioned in case files may be included.
<b>Race, ethnicity, or citizenship</b>	X	A, B, C, and D	Race, ethnicity or citizenship of individuals mentioned in case files may be included.
<b>Religion</b>	X	A, B, C, and D	Religion of individuals mentioned in case files may be included.
<b>Social Security Number (full, last 4 digits or otherwise truncated)</b>	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.

(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
<b>Tax Identification Number (TIN)</b>	X	A, B, C, and D	Tax Identification Number (TIN) of individuals mentioned in case files may be included.
<b>Driver's license</b>	X	A, B, C, and D	Driver's licenses of individuals mentioned in case files may be included.
<b>Alien registration number</b>	X	A, B, C, and D	Alien registration numbers of individuals mentioned in case files may be included.
<b>Passport number</b>	X	A, B, C, and D	Passport numbers of individuals mentioned in case files may be included.
<b>Mother's maiden name</b>	X	A, B, C, and D	Mother's maiden name of individuals mentioned in case files may be included.
<b>Vehicle identifiers</b>	X	A, B, C, and D	VINs, and license plate numbers mentioned in case files may be included.
<b>Personal mailing address</b>	X	A, B, C, and D	Personal mailing addresses of individuals mentioned in case files may be included.
<b>Personal e-mail address</b>	X	A, B, C, and D	Personal e-mail addresses of individuals mentioned in case files may be included.
<b>Personal phone number</b>	X	A, B, C, and D	Personal phone numbers of individuals mentioned in case files may be included.
<b>Medical records number</b>	X	A, B, C, and D	Medical records numbers of individuals mentioned in case files may be included.
<b>Medical notes or other medical or health information</b>	X	A, B, C, and D	Medical notes or other medical or health information mentioned in case files may be included.
<b>Financial account information</b>	X	A, B, C, and D	Financial account information of individuals mentioned in case files may be included.
<b>Applicant information</b>	X	A, B, C, and D	Applicant information of individuals mentioned in case files may be included.
<b>Education records</b>	X	A, B, C, and D	Education records of individuals mentioned in case files may be included.
<b>Military status or other information</b>	X	A, B, C, and D	Military status or other information 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
<b>Employment status, history, or similar information</b>	X	A, B, C, and D	Employment status, history, or similar information of individuals mentioned in case files may be included.
<b>Employment performance ratings or other performance information, e.g., performance improvement plan</b>	X	A, B, C, and D	Performance improvement plan, warnings or reprimands of individuals mentioned in case files may be included.
<b>Certificates</b>	X	A, B, C, and D	Certificates mentioned in case files may be included.
<b>Legal documents</b>	X	A, B, C, and D	Legal documents mentioned in case files may be included.
<b>Device identifiers, e.g., mobile devices</b>	X	A, B, C, and D	Device identifiers mentioned in case files may be included.
<b>Web uniform resource locator(s)</b>	X	A, B, C, and D	Web uniform resource locator(s) mentioned in case files may be included.
<b>Foreign activities</b>	X	A, B, C, and D	Foreign activities of individuals mentioned in case files may be included.
<b>Criminal records information, e.g., criminal history, arrests, criminal charges</b>	X	A, B, C, and D	Criminal records information of individuals mentioned in case files may be included.
<b>Juvenile criminal records information</b>	X	A, B, C, and D	Juvenile criminal records information of individuals mentioned in case files may be included.
<b>Civil law enforcement information, e.g., allegations of civil law violations</b>	X	A, B, C, and D	Civil law enforcement information mentioned in case files may be included.
<b>Whistleblower, e.g., tip, complaint, or referral</b>	X	A, B, C, and D	Whistleblower information mentioned in case files may be included.
<b>Grand jury information</b>	X	A, B, C, and D	Grand jury information mentioned in case files may be included.
<b>Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information</b>	X	A, B, C, and D	Information concerning witnesses to criminal matters mentioned in case files may be included.
<b>Procurement/contracting records</b>	X	A, B, C, and D	Procurement/contracting records mentioned in case files may be included.
<b>Proprietary or business information</b>	X	A, B, C, and D	Proprietary or business 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
<b>Location information, including continuous or intermittent location tracking capabilities</b>	X	A, B, C, and D	Location information mentioned in case files may be included.
<i>Biometric data:</i>			
- <b>Photographs or photographic identifiers</b>	X	A, B, C, and D	Photographs or photographic identifiers of individuals mentioned in case files may be included.
- <b>Video containing biometric data</b>	X	A, B, C, and D	Video containing biometric data of individuals mentioned in case files may be included.
- <b>Fingerprints</b>	X	A, B, C, and D	Fingerprints of individuals mentioned in case files may be included.
- <b>Palm prints</b>	X	A, B, C, and D	Palm prints of individuals mentioned in case files may be included.
- <b>Iris image</b>	X	A, B, C, and D	Iris images of individuals mentioned in case files may be included.
- <b>Dental profile</b>	X	A, B, C, and D	Dental profiles of individuals mentioned in case files may be included.
- <b>Voice recording/signatures</b>	X	A, B, C, and D	Voice recordings/signatures of individuals mentioned in case files may be included.
- <b>Scars, marks, tattoos</b>	X	A, B, C, and D	Scars, marks, tattoos of individuals mentioned in case files may be included.
- <b>Vascular scan, e.g., palm or finger vein biometric data</b>	X	A, B, C, and D	Vascular scans of individuals mentioned in case files may be included.
- <b>DNA profiles</b>	X	A, B, C, and D	DNA profiles of individuals mentioned in case files may be included.
- <b>Other (specify)</b>	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.
<i>System admin/audit data:</i>			
- <b>User ID</b>	X	A, B, C, and D	User ID of DOJ users, corporate counsels, litigators and government attorneys.
- <b>User passwords/codes</b>	X	A, B, C, and D	User passwords/codes of DOJ users, corporate counsels, litigators and government attorneys.

(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
- 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	Given the varied nature of civil and criminal litigation, it is not possible to identify all of the categories of PII that could be handled in Everlaw.

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

<b>Directly from the individual to whom the information pertains:</b>					
In person	X	Hard copy: mail/fax	X	Online	X
Phone	X	Email	X		
Other (specify): This would only apply in a Pro Se Litigant Case.					

<b>Government sources:</b>					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
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): Agreement Between the Government of the United States and the Government of Canada Regarding the Application of their Competition and Deceptive Marketing Practices; U.S.-Canada Cooperation Agreement; Migrant Protections Protocol; and additional information sharing agreements that further the mission of DOJ					

<b>Non-government sources:</b>					
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.					

**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	EOUSA users securely view, process, analyze and report upon information and data related to a case. The information is reviewed and used to build and support their cases in a court of law.
DOJ Components	X		X	DOJ component users securely view, process, analyze and report upon information and data related to a case. The information is reviewed and used to build and support their cases in a court of law.
Federal entities	X		X	Federal users securely view, process, analyze and report upon information and data related to a case. The information is reviewed and used to build and support their cases in a court of law.

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.
State, local, tribal gov't entities	X		X	State, local and tribal government entities securely view, process, analyze and report upon information and data related to a case. The information is reviewed and used to build and support their cases in a court of law.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X		X	Access is provided to counsel, parties, and witnesses, when the data is too large to otherwise transmit electronically or in hard copy.  Court administrators may be provided access to limited materials in the system as required by the courts.
Private sector	X		X	Private sector, namely expert witnesses and entities, are provided access to the system in support of litigation for file sharing and data analysis.
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.*

Not Applicable

**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 except in Pro Se Litigant cases. The information is part of case files required for 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 modified at 82 Fed. Reg. 24147(Jan. 22, 1988), available at: <https://www.justice.gov/opcl/docs/usa-005-53fr1864.pdf>.
- DOJ/USA-007, “Criminal Case Files,” last modified at 82 Fed. Reg. 24147(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 directly collected from individuals except in Pro Se Litigant cases. Rather, it is information gathered from a variety of sources, including opposing counsel and investigators. The information uploaded to Everlaw consist of records used by USAOs in support of cases in a court of law. Thus, individuals do not generally have the opportunity to opt out of the collection, use, or dissemination of their information from USALMA-c.

**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.*

Individuals may request access to any information in the system pertaining to them by following instructions on this site for submitting a FOIA request:  
<https://www.justice.gov/usao/resources/making-foia-request>.

Additional information regarding access to information may be found in the following SORNs:

- DOJ/USA-005, “Civil Case Files,” last modified at 82 Fed. Reg. 24147(Jan. 22, 1988), available at: <https://www.justice.gov/opcl/docs/usa-005-53fr1864.pdf>.
- DOJ/USA-007, “Criminal Case Files,” last modified at 82 Fed. Reg. 24147(Jan. 22, 1988), available at: <https://www.justice.gov/opcl/docs/usa-007-53fr1864.pdf>.

**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	<p><b>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):</b> The existing USALMA-c ATO expires 1/15/27.</p> <p><b>If an ATO has not been completed, but is underway, provide status or expected completion date:</b> Not Applicable</p> <p><b>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:</b> POA&amp;M #38210 has been created to track the creation of the USALMA-c PIA.</p>
	<p><b>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:</b> N/A</p>
X	<p><b>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:</b> USALMA-c 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. The implemented controls undergo control assessments on an annual basis to ensure they are properly implemented. Assessment includes vulnerability testing, compliance monitoring, and control evaluation.</p>
X	<p><b>Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:</b> The implemented controls undergo control assessments on an annual basis to ensure they are properly implemented. Assessment includes vulnerability testing, compliance monitoring, and control evaluation.</p>
X	<p><b>Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:</b> USALMA-c audit logs are reviewed weekly by the ISSO. If any abnormal activity is identified, it is reported to the Security Officer and the team for further review.</p>
X	<p><b>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.</b></p>
X	<p><b>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:</b> General information security and privacy training and training specific to the system for authorized users within the Department. External users are required to complete the Litigation</p>

	Technology Help Desk (LTHD) rules of behavior prior to being provided access to the Everlaw application.
--	--

**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 in place ensure that only authorized users have access to the information collected, in addition to only being granted the privileges necessary to perform their duties. Additionally, safeguards are in place that ensure that unauthorized access to the system is not granted and the risk of unauthorized disclosure of the information within the system is minimized. USALMA-c is integrated with USAAuth, and users use Single Sign-On to access the application. All login actions are audited to ensure that no unauthorized users have been granted access to the system and all audit logs are reviewed on a weekly basis by the ISSO. An open session within the information system is also 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 USALMA-c system is maintained for as long as needed by authorized DOJ users, corporate counsel, litigators, and government attorneys and is subject to the respective retention periods that govern it, 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>).

USALMA-c follows the DOJ Network Account Records Management USAPP 3-13.300.004 procedures that have been developed to ensure that electronic copies are not retained beyond the retention period established for the original records and will be disposed of in accordance with the requirements outlined in the above procedures.

## **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).**

\_\_\_\_\_ No.        X   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 modified at 82 Fed. Reg. 24147(Jan. 22, 1988), available at: <https://www.justice.gov/opcl/docs/usa-005-53fr1864.pdf>.
- DOJ/USA-007, “Criminal Case Files,” last modified at 82 Fed. Reg. 24147(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 complete 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 Litigation Technology Service Center (LTSC) 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 ISSO on a weekly basis to identify any unauthorized user actions, such as data exfiltration or modification/deletion.

Additionally, all security controls are tested annually for 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.