Homegrown Canna VA Security Division

PRIVACY PLAN

Version: 1.0
Date: 09/03/2024

Contents

RECORD OF CHANGES AND REVIEW

NUMBER	DATE	DESCRIPTION	ENTERED BY
1.0	10/5/2023	First Draft	Security Research Group

Purpose & Scope

The purpose of the Homegrown Canna VA Privacy Program Plan is to provide an overview of the Companies privacy program. This plan highlights:

- A description of the structure of the privacy program;
- The resources dedicated to the privacy program;
- The role of the Senior Officials and other privacy officials and staff;
- The strategic goals and objectives of the privacy program;
- The program management controls in place to meet applicable privacy requirements and manage privacy risks; and
- Any other information deemed necessary by Homegrown Canna VA privacy program.

Overview of the Privacy Program

Mission Statement

Homegrown Canna VA is committed to safeguarding personal privacy. Individual trust in the privacy and security of personally identifiable information (PII) is a foundation of trust in government and commerce in the 21st Century. As an employer, a collector of data on individuals and companies, Homegrown Canna VA strives to be a leader in best privacy practices and privacy policy. To further this goal, we assign a high priority to privacy consideration in all systems, programs, and policies.

1.1 *Strategic Goals and Objectives for Privacy*

Homegrown Canna VA Privacy Program supports five core missions as articulated in the Innovation, Equity, and Resilience, Strengthening American competitiveness in the 21st Century, 2022 – 2026 Strategic Plan, as well as the important cross-cutting goal to mature and strengthen economic growth by preserving privacy, oversight, and transparency in the execution of all activities. To accomplish the strategic outcomes, there are four Privacy Program goals, each supported by specific and measurable objectives:

GOAL 1

❖ Foster a culture of privacy and disclosure and demonstrate leadership through policy and partnerships.

In promoting economic growth, Homegrown Canna VA is entrusted to collect personal information from business, citizens. We are obligated to collect only the information that is necessary to carry out our missions and protect this data from misuse. Our core mission is to respect and protect individual privacy rights. We also have a duty to be accessible, transparent to our customers. Homegrown Canna VA privacy and disclosure professionals are integrated into the operations of Operating Unit. It is through this framework that the Homegrown Canna VA Privacy Program is able to maintain one of its most valuable assets: the public trust.

- ✓ Objective 1.1 – Support Homegrown Canna VA unity of effort by representing privacy and disclosure interests in Company governance.
- ✓ Objective 1.2 – Provide guidance and issue policies related to privacy by leveraging the expertise of Privacy Officers and Privacy Points of Contact from across the Company using issue-based governance bodies.
- ✓ Objective 1.3 – Leverage the expertise of oversight and advisory bodies, advocates, and privacy experts from the private sector to foster dialogue and learn about emerging issues.

GOAL 2

❖ Provide outreach, education, training, and reports to promote privacy and transparency.

Privacy practices, principles, and protections are implicated in Homegrown Canna VA approach to implementing all of its missions. Privacy and the Homegrown Canna VA missions are not traded or balanced, but rather are integrated in a manner that honors our core values. Homegrown Canna VA Privacy Program ensures that Homegrown Canna VA privacy protections and policies are understood by every Homegrown Canna VA employee through education and training and made known to the privacy community and public at large through extensive outreach.

- ✓ Objective 2.1 – Ensure consistent application of privacy and disclosure requirements, and accountability across the Company.
- ✓ Objective 2.2 – Develop and deliver targeted and effective privacy training material to Homegrown Canna VA personnel and other stakeholders through targeted educational and outreach opportunities tailored to Homegrown Canna VA's broad constituency.
- ✓ Objective 2.3 – Pursue proactive, timely disclosure of information about Homegrown Canna VA programs, operations, systems, and policies in a manner that is easily accessible to oversight bodies.
- ✓ Objective 2.5 – Promote Company privacy practices to international partners to advance the Fair Information Practice Principles (FIPPs) and build the confidence necessary to fulfill Homegrown Canna VA mandate as it relies on international cooperation.

GOAL 3

❖ Conduct robust compliance and oversight programs to ensure adherence with federal privacy and disclosure laws and policies in all Homegrown Canna VA activities.

Privacy protections are firmly embedded into the lifecycle of Homegrown Canna VA programs and systems. In addressing new risks or adopting new and integrated approaches to protecting individual privacy, the privacy enterprise must identify early on any potential for infringement of core privacy values and protections and address that risk accordingly. When issues are identified and resolved early, it helps ensure that programs and services provide the maximum public benefit with the least possible privacy risk.

- ✓ Objective 3.1 – Review, assess, and provide guidance to Homegrown Canna VA programs, systems, projects, information sharing arrangements, and other initiatives to reduce the impact on privacy and ensure compliance.
- ✓ Objective 3.2 – Promote privacy best practices and guidance to Homegrown Canna VA information sharing activities.
- ✓ Objective 3.3 – Ensure that complaints and incidents at Homegrown Canna VA are reported systematically, processed efficiently, and mitigated appropriately in accordance with federal and Homegrown Canna VA privacy policies and procedures.

- ✓ Objective 3.4 – Evaluate Homegrown Canna VA programs and activities for compliance with privacy and disclosure laws.
- ✓

GOAL 4

- ✓ Develop and maintain the best privacy and disclosure professionals.

The human capital of Homegrown Canna VA is widely regarded as among the most talented privacy and disclosure professionals in the trade. This top tier talent is crucial to Homegrown Canna VA continued ability to implement its missions and to its success in maintaining the public trust. These professionals have continuously demonstrated agility in responding to new priorities and fiscal environments. Providing support, opportunities for professional growth and development, and a workplace environment in which they are valued are all crucial to recruiting and retaining a high performing workforce.

- ✓ Objective 4.1 – Reward exceptional employee performance and recognize individual contributions to advancing the office mission.
- ✓ Objective 4.2 – Support employee development and emphasize the role of training and professional development in performance planning.
- ✓

Privacy Office Organization

The Privacy Officer provides oversight and management of the Homegrown Canna VA Privacy Program. Andres Puel serves as Director of Chief Privacy Officer (CPO). The CPO is the Company's key policy advisor on implementing the Privacy Act of 1974, 5 U.S.C. §552a, and the privacy provisions of the Federal Information Security Modernization Act (FISMA) of 2014, and of the E-Government Act of 2002. The responsibilities of the CPO include:

- Serving as the Company's senior policy authority on matters relating to the public disclosure of information, and advising on privacy issues related to informed consent, disclosure risks, and data sharing;
- Developing and overseeing implementation of Company-wide policies and procedures relating to the Privacy Act, and assures that personal information contained in Privacy Act systems of records is handled in compliance with its provisions;
- Communicating the Company's privacy vision, principles, and policies internally and externally;
- Ensuring the Company considers and addresses the privacy implications of all Homegrown Canna VA regulations and policies, and leading the Company's evaluation of the privacy implications of legislative proposals, congressional testimony, and Office of Management and Budget (OMB) guidance;
- Advocating strategies for data and information collection and dissemination, to ensure Company privacy policies and principles are reflected in all operations;
- Ensuring Company policies and procedures regarding information protection are compliant with statutory and government-wide policy requirements, verifying Company adherence to relevant information

protection policies and procedures, and continually striving to identify and implement privacy best practices;
- Coordinating the Company process for reviewing and approving Privacy Impact Assessments (PIAs) to ensure compliance with the E-Government Act;
- Managing privacy risks associated with Homegrown Canna VA activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII;
- Ensuring the appropriate training and education regarding privacy laws, regulations, policies and procedures concerning the handling of personal information are afforded to employees and vendors with access;
- Working with the Company's stakeholders to ensure vendors with access to PII engaging in business with the Company abide by the Federal privacy requirements; and
- Facilitating and negotiating agreements with senior management, and establishing relationships with partners in private industry and other federal agencies to foster the development and sharing of privacy-related best practices; and partners with the Office of the Chief Information Officer to ensure all aspects of the Privacy Program are incorporated into the Company's enterprise infrastructure, IT, and IT security program.

Chief Privacy Officers

The Homegrown Canna VA Privacy Program is implemented within Homegrown Canna VA and by the CEO. A Chief Privacy Officer is designated to represent the Company.

The Homegrown Canna VA CEO is ultimately responsible for ensuring that privacy interests are protected and that PII is managed responsibly within the Company. To ensure that Homegrown Canna VA effectively carry out the privacy-related functions described in law and policies, the Homegrown Canna VA requires the head of the Company designate a CPO who has Company-wide responsibility and accountability for the Company's privacy program. The role and designation of the CPO shall be governed by the following requirements:

- Position. The CPO shall be a senior official who serves in a central leadership position at the Company, has visibility into relevant Company operations, and is positioned highly enough within the Company to regularly engage with other Company leadership, including the head of the Company.

- Expertise. The CPO shall have the necessary skills, knowledge, and expertise to lead and direct the Company's privacy program and carry out the privacy-related functions described in law and Homegrown Canna VA policies.

- Authority. The CPO shall have the necessary authority at the Company to lead and direct the Company's privacy program and carry out the privacy-related functions described in law and Homegrown Canna VA policies.

Homegrown Canna VA PII Breach Response Task Force

The Homegrown Canna VA PII Breach Response Task Force is responsible for providing in-depth analysis and recommendations for an appropriate response to PII breaches that may cause significant harm to individuals or the Company. The Homegrown Canna VA PII Breach Response Task Force is chaired by the CPO. Members include the Chief Executive Officer (CEO), Chief Financial Officer (CFO), General Counsel, Chief Information Officer (CIO).

The CPO determines when to convene Task Force meetings for moderate risk, high risk, and major PII breach incidents. More information may be found in the Homegrown Canna VA Privacy Act, Personally Identifiable Information (PII), and Business Identifiable Information (BII) Breach Notification Plan.

Privacy Workforce Management

The CPO assesses and addresses the hiring, training, and professional development needs of the Company with respect to privacy, including providing input into the performance of employees who function in the capacity of work for the CPO for the Company out of any operating unit. Additionally, the CPO coordinates with the Chief Information Officer and Chief Administration officer to maintain and enhance a current workforce planning process, maintain workforce skills, recruit and retain privacy and IT professionals, develop a set of competency requirements for staff, and ensure managers are aware of flexible hiring authorities.

Fair Information Practice Principles

The Homegrown Canna VA Privacy Program adheres to the Fair Information Practice Principles (FIPPs). Homegrown Canna VA uses these principles when evaluating information systems, processes, programs, and activities that affect individual privacy. The FIPPs include:

- Access and Amendment – Individuals are provided with appropriate access to PII and the opportunity to correct or amend PII.
- Accountability – Homegrown Canna VA ensures compliance with these principles and applicable privacy requirements by monitoring, auditing, and documenting compliance. In addition, the roles and responsibilities with respect to PII for individuals are defined and appropriate training is provided to individuals who have access to PII.
- Authority – When the company is to create, collect, use, process, store, maintain, disseminate, or disclose PII, the appropriate authorities are documented.
- Minimization – When the company is to create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish the legally authorized purpose. The PII is

maintained for as long as is necessary to accomplish the purpose.

- Quality and Integrity – When the company is to create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
- Individual Participation – Individuals are involved in the process of using PII and, to the extent practicable, individual consent is granted for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Individuals may address concerns or complaints to the Homegrown Canna VA Privacy Officer.
- Purpose Specification and Use Limitation – Homegrown Canna VA will provide notice of the specific purpose for which PII is collected and only use, process, store, maintain, disseminate, or disclose PII for the purpose that is explained in the notice.
- Security – Administrative, technical, and physical safeguards are established to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.
- Transparency – Homegrown Canna VA will provide clear and accessible notice regarding the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

Privacy Risk Management Framework

Homegrown Canna VA follows the process described in NIST SP 800-37 that incorporates information security and privacy risk management activities into the system development life cycle. This process includes:

- Categorizing each information system and the information processed, maintained, and transmitted by each system based on a mission or business impact analysis using NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
  1) The FIPS 199 security impact category is not the same as the NIST SP 800-122 PII Confidentiality Impact Level. The categorization of PII is found in Appendix B.
- Selecting and implementing privacy and security controls and documenting how these controls are deployed for each information system;
- Assessing the privacy and security controls, including privacy continuous monitoring; and
- Obtaining CPO approval prior to the 1) operation of a new system which will collect, process, share, and/or store PII; and 2) authorize changes on a legacy PII processing, sharing, and/or storage system which will create new privacy risks, including adding a new collection of PII.

Privacy Control Requirements/Continuous Monitoring Strategy

The Homegrown Canna VA ensures compliance with all applicable statutory, regulatory, and policy requirements. The Homegrown Canna VA implements the NIST SP 800-53, Rev 4 baseline of security and privacy controls, including Privacy

Overlays. The Homegrown Canna VA adheres to Section 208 of the E-Government Act of 2002, which requires Companies to conduct Privacy Threshold Analyses (PTAs) and PIAs for electronic information systems and collections. In addition, the Homegrown Canna VA meets Privacy Act System of Records Notice (SORN) requirements.

Homegrown Canna VA Appendix C Control Allocation Table

The Homegrown Canna VA CPO designates which privacy controls the Company will treat as program management, common, information system-specific, and hybrid controls. Privacy program management controls are controls that are generally implemented at the agency level and essential for managing the agency's privacy program. Common controls are controls that are inherited by multiple information systems. Information system-specific controls are controls that are implemented for a particular information system or the portion of a hybrid control that is implemented for a particular information system. Hybrid controls are controls that are implemented for an information system in part as a common control and in part as an information system-specific control. The determination as to whether a privacy control is a common, hybrid, or information system-specific control is based on context. The Appendix C Control Allocation Table is found in Appendix C.

Homegrown Canna VA Privacy Overlays

The Homegrown Canna VA Privacy Program leverages privacy overlays established for national security systems as guidance when selecting/assessing effectiveness of privacy protections. According to NIST SP 800-53, Revision 5, an overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The purposes of the privacy overlays include providing standard security and privacy control baselines for systems containing PII, ensuring integration of privacy considerations into the system development life cycle and security processes in the early stages, and providing guidance for privacy requirements for protected health information. Summarized information on implementing privacy overlays is found in Appendix D.

Privacy Threshold Analysis (PTA)

A PTA is a questionnaire used to determine if a system contains PII, whether a PIA is required, whether a SORN is required, and if any other privacy requirements apply to the information system. A PTA is completed when proposing a new information technology system through the budget analysis process that collects, stores, or processes identifiable information; when developing or significantly modifying such a system; or when proposing a new electronic collection of identifiable information. A PTA determines if a PIA is required. The PTA Template is found in Appendix E.

Homegrown Canna VA also has a PTA for information collections and forms.

Privacy Impact Assessment (PIA)

A PIA is an analysis of how information in identifiable form is collected, maintain,

stored, and disseminated, in addition to examining and evaluating the privacy risks and the protections and processes for handling information to mitigate those privacy risks. A PIA is conducted before:

A. Developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form, from or about, members of the public; or
B. Initiating a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

If a PIA is required, the CPO and CEO work closely with the CIO to complete the PIA Template (Appendix G). Also, a Controls Assessment Worksheet (C) which identifies the status of the security and privacy controls applicable to the PII Confidentiality Impact Level must be completed and approved by the Company's Chief Executive Officer. Once these Homegrown Canna VA documents are complete and fully signed by the certifying officials, the CPO submits the PTA, PIA, and Controls Assessment Worksheet to the CEO for review.

Contractors and Third Parties

The Homegrown Canna VA ensures contractors and third parties that: 1) create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information on behalf of the Company; or 2) operate or use information systems on behalf of the Company, comply with the mandated privacy requirements. The Homegrown Canna VA Privacy Program ensures that the applicable privacy clauses, below from the FAR, are included in the terms and conditions in contracts and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of information in the possession of the Company:

- FAR Subpart 4.19 – Basic Safeguarding of Covered Contractor Information Systems
  - FAR Clause 52.204-21
- FAR Subpart 24.1 Protection of Individual Privacy
  - FAR Clause 52.224-1 "Privacy Act Notification"
  - FAR Clause 52.224-2 "Privacy Act"
- FAR 39.101 – Acquisition of Information Technology-General-Policy
- FAR 39.105 – Acquisition of Information Technology-General-Privacy
  - FAR Clause 52.239-1 "Privacy or Security Safeguards"
- FAR Subpart 27.4 – Rights in Data and Copyrights

Privacy Act Statement

The Homegrown Canna VA ensures that a compliant Privacy Act Statement is provided or available when collecting PII. The Privacy Act Statement is provided on the collection instrument, on a poster that is visible to the individual, or on a separate form that can be retained by the individual prior to the actual collection. A Privacy Act Statement provides an individual with the following:

- Companies legal authority to collect the information, such as a statute, executive order, and/or regulation;
- Purpose(s) for collecting the information and how it will be used;
- Routine uses of the information, which describes to whom the Company may disclose information outside of the Company and for what purposes; and
- Whether providing the information is mandatory or voluntary, along with the effects, if any, on the individual of not providing all or any part of the information requested.

Overview of Requirements for Handling and Protecting Personally Identifiable Information (PII)/Business Identifiable Information (BII)

Handling and safeguarding PII in the Company's possession is fundamental to ensure the public's trust. At the Company, BII must be similarly protected as PII, in accordance with applicable laws. In an effort to protect all data, the Company Privacy Standards for Homegrown Canna VA Data Loss Prevention (DLP) Security Tools establishes a requirement for Homegrown Canna VA to configure their DLP security tools to implement privacy control capabilities that enhance privacy protections and reduce PII breaches within the Company.

Recognizing Personally Identifiable Information (PII)

PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual. Some examples of PII include name, Social Security number (SSN), biometric records, etc. which alone, or combined with other personal or identifying information, such as date and place of birth, mother's maiden name, etc. can be linked to a specific individual.

Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in harm, embarrassment, inconvenience, or unfairness to an individual. The following types of PII are considered sensitive when associated with an individual:

- SSN (including in truncated form);
- Place of birth;
- Date of birth;
- Mother's maiden name;
- Biometric information;
- Medical information (excluding brief references to absences from work);
- Personal financial information;
- Credit card/purchase card account numbers;
- Passport numbers;
- Potentially sensitive employment information (e.g., performance ratings, disciplinary actions, results of background investigations);
- Criminal history; or
- Information that may stigmatize or adversely affect an individual.

Context of information is important. The same types of information can be sensitive or non- sensitive depending upon the context. For example, a list of names and telephone numbers for the Company's softball roster is very different from a list of names and telephone numbers for individuals being treated for an infectious disease.

Recognizing Business Identifiable Information (BII)

BII is information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." This information is exempt from automatic release under the FOIA exemption. "Commercial" is not confined to records that reveal "basic commercial operations," but includes any records or information in which the submitter has a "commercial interest" and can include information submitted by a nonprofit entity; or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C. 9).

Commercial or financial information is considered confidential if the submitter customarily keeps the information private or closely held, and the government provides an express or implied assurance of confidentiality when the information is shared with the government. Examples of BII include financial information provided in response to requests for economic census data, business plans and marketing data provided to participate in trade development events, commercial and financial information collected as part of export enforcement actions, proprietary information provided in support of a grant application or related to a federal acquisition action, and financial records collected as part of an investigation.

Minimizing the Collection of PII/BII

The Privacy Act of 1974 requires that Federal agencies maintain only relevant and necessary information about individuals..

The Homegrown Canna VA maintains a Company-wide inventory of PII/BII holdings and uses the PTA, and PIA certification process to identify reduction opportunities and to ensure, to the maximum extent practicable, that such holding is accurate, relevant, timely, and complete.

Handling and Transmitting PII/BII

PII requires strict handling guidelines due to the nature of the data and the increased risk to an individual if data were to be compromised. Ways of handling PII/BII include:

- Encrypt sensitive PII/BII on computers, media, and other devices;
- Lock or log off unattended computer systems;
- Destroy sensitive paper PII/BII by shredding or using burn bags;
- Delete sensitive electronic PII/BII by emptying computer "recycle bin";
- Store sensitive PII/BII on secure Federal Government systems only; and
- Secure sensitive paper PII/BII data by locking in desks and filing cabinets.

Sensitive PII/BII may be distributed or released to other individuals if it is within the

scope of their official duties and they have a need to know. If sensitive PII/BII is electronically transmitted, it must be protected by secure methodologies, such as encryption, Public Key Infrastructure, or secure sockets layer. When in doubt, treat PII as sensitive. The transmission of sensitive PII and BII must be kept to a minimum, even if it is protected by secure means.

Other ways for communicating, sending, and receiving sensitive PII/BII include:

- Facsimile – When faxing information, include an advisory statement about the contents on the cover sheet and notify the recipient before and after transmission. Exception: According to Homegrown Canna VA Acquisition Manual 1313.301, Homegrown Canna VA purchase card holders shall not transmit purchase card information over a facsimile machine.
- Mail – Physically secure sensitive PII/BII when in transit by sealing it in an opaque envelope or container, and mail using First Class or Priority Mail, or a commercial delivery service. Redact SSNs from documents where feasible. When full redaction is not feasible, partially redact to create a truncated SSN. Do not mail, or send by courier sensitive PII/BII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted.
    - Inclusion of SSNs on documents when mailing:
        - The following conditions must be met for the inclusion of an unredacted (full) SSN or partially redacted (truncated) SSN on a responsive document:
            (i) Must be required or authorized by law; and
            (ii) Must be determined by the CPO and DPAO to be necessary to fulfill a compelling Company business need.
        - The following requirements apply when the Homegrown Canna VA mails a document containing a full or truncated SSN:
            (i) The document must be identified on the Un-redacted SSN Mailed Homegrown Canna VA document listing
            (ii) The signature of the recipient is required upon delivery; and
            (iii) The full SSN or truncated SSN must not be visible from the outside of the envelope or package.
- Hard Copy – Hand-deliver documents containing sensitive PII/BII if needed. Do not leave sensitive PII/BII unattended on printers, facsimile machines, or copiers.

Breach Incident Response and Management

Homegrown Canna VA has a duty to appropriately safeguard all PII in its possession and to prevent compromise of this information in order to maintain the public's trust. The Privacy Act, PII, and BII Breach Notification Plan serves to inform all employees, vendors with access of their obligation to protect PII and establish procedures to define how to prepare for and respond to any breach incidents.

Additionally, the *Procedures on Notifying Management Officials of Individuals Who Fail to Safeguard Sensitive PII* can be used by the CPO to ensure managers, supervisors, and/or contracting officer representatives are made aware of a PII breach incident in a timely manner.

OMB Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, provides the policy agencies to prepare for and respond to a breach of PII. The CPO and the CIO will work together to ensure a PII breach is expeditiously reported, handled, and closed appropriately.

CPOs must ensure:

- All PII breach incidents are reported to the CPO and the CEO within one (1) hour of discovery/detection.
- All PII breach incidents are under investigation within 48 hours of the incident discovery/detection.
- A follow-up report is completed and submitted to the CEO and the CPO.
- All corrective/remedial actions for each PII breach incident are confirmed completed prior to the close-out of a low risk PII incident. CPO concurrence must be granted prior to the close-out of a moderate risk, high risk, and/or Major PII breach incident.

CPOs must complete and submit a Summary Incident Report (H) to the CEO within the following timeline:

- Major PII Incident – within 24 hours
- High Risk PII Incident – within three (3) work days
- Moderate Risk PII Incident – within three (3) to five (5) work days

The CPO provides notification of all cyber related (electronic) PII breach incidents with confirmed loss of confidentiality, integrity, or availability to the CEO within one (1) hour of being reported. If an assessment has been made that a PII breach incident constitutes a Major incident, the CPO reports the designation to CEO as soon as the Company has a reasonable basis to conclude that such a PII breach incident has occurred. The CPO reports all non-cyber related (paper) incidents to the CEO within one (1) hour of a confirmed PII breach incident.

Additionally, the CPO convenes the Homegrown Canna VA PII Breach Response Task Force annually to hold a tabletop exercise. The purpose of the tabletop exercise is to test the Company's Breach Response Plan and to help ensure that members of the team understand their specific roles and are familiar with the Breach Response Plan. Lessons learned from the tabletop exercise are discussed with the Task Force, as well as the Homegrown Canna VA Board.

Awareness and Training

As Homegrown Canna VA strives to be a leader in best privacy practices and privacy policy, the Company requires a mandatory privacy performance element in every employee performance plan. This ensures high priority is assigned to privacy considerations in all systems, programs, and policies. The Homegrown Canna VA Privacy Training Program promotes maximum employee and vendor with access understanding and adherences to the FIPPs. Based on the need, different levels of training are offered or are mandatory for employees and contractors.

Homegrown Canna VA conducts activities promoting privacy and security awareness, such as Privacy Day, Sunshine Week, Cybersecurity Awareness Day, and Security Awareness Day. During these events, the following privacy brochures are discussed and distributed to employees, contractors, and visitors:

- How to Protect PII and BII when Transmitting to Authorized Users
- PII Breach Incident Reporting
- Privacy Impact Assessments
- Homegrown Canna VA's Quick-Start Guidance for Moving Sensitive PII/BII

New Employee Orientation Training

New employee orientation sessions across the Company include presentations on how to handle privacy protected information and Privacy Act information protection requirements. Privacy Slide which provide definitions and examples of PII and BII, along with step by step procedures on how to use the Company's suite of encryption and secure file transfer technologies to protect sensitive PII transmitted electronically are distributed to all new employees during orientation.

Conclusion

The Homegrown Canna VA is committed to safeguarding PII/BII. The Homegrown Canna VA Privacy Program intends to use all methods of regulation, policy, guidance, and principles to further this objective across the Company of Homegrown Canna VA. Privacy considerations are a part of all levels of decision-making in an effort to continuously build a culture of trust and privacy throughout each Company.

Appendices

Appendix A – Authorities, Memoranda, Policies, and Guidance

Authorities

- Privacy Act of 1974, 5 U.S.C. §552a
- Federal Information Security Modernization Act of 2014
- Freedom of Information Act (FOIA)
- Trade Secrets Act
- Paperwork Reduction Act of 1995
- Children's Online Privacy Protection Act of 1998
- Homegrown Canna VA Privacy Policy

Appendix B – Categorizing PII

Categorizing Personally Identifiable Information (PII)

This document adopts use of the OMB recommended Best Judgment Standard and follows a twostep approach regarding categorizing information about individuals: (i) consider whether the information is within scope of the definition of PII, and (ii) consider the sensitivity of the PII in the context in which it appears. The sections below facilitate completion of the first step of OMB's approach by identifying PII and PHI.[3] Implementation of the second step of OMB's approach within Homegrown Canna VA is discussed below under "Categorizing PII Using NIST SP 800-122 defined Confidentiality Impact Levels."

IMPORTANT NOTE

The PII confidentiality impact level is not the same, and should not be confused with, the security objective of confidentiality for the system.

Identifying PII

OMB memoranda collectively define PII as (i) data elements which alone can distinguish or trace an individual's identity, i.e., unique identifiers; (ii) non-PII that becomes PII when it identifies an individual in aggregate, i.e., compilation effect; and (iii) non-PII that becomes PII when combined with a unique identifier or data elements that have aggregated to become PII, i.e., by association. Data elements which meet one or more of these criteria are PII and should be protected.

(i) Data elements which alone can distinguish or trace an individual's identity Many types of data elements can uniquely identify an individual without the need to first combine it with other data elements. This category of PII is most commonly encountered when a unique number or other[5] identifier is assigned to an individual (e.g., name, Social Security Number, passport number, or driver's license number) or with respect to unique identifiers that are part of an individual's

---

To protect PII within an information system, system owners must be able to locate and identify the PII and should recognize that inclusion of PII in a system may not be immediately apparent. System owners should be familiar with all aspects of an information system. Examples of where PII may be identified for a system include the data dictionary, the architecture for the data store(s), or the data store(s) themselves. For existing systems, current privacy documentation, such as Privacy Impact Assessments (PIAs) and system of records notices (SORNs), may provide insight into the types of PII in a system, but they may be documented at a higher level of categories or types than is

necessary for the categorization of system information and determining privacy risk for the purposes of implementing the Privacy Overlays.

Unique identifiers alone can be used to identify a specific individual.

(ii) Non-PII becomes PII when it is combined with other information to identify an individual

Akin to the compilation effect, data elements which alone do not identify an individual and are not PII can become PII if, when combined, they uniquely identify an individual. [6] For example, a zip code, birthdate, or gender alone will not identify someone. However, if these three elements are associated with each other they narrow the scope of reference and enable either identification or re-identification of the individual, thereby making these elements PII.

Accordingly, prevention against re-identification[5] under the compilation effect extends beyond the mere removal of name and social security number. To ensure that information does not compile to become PII, refer to one of the accepted methods of data de- identification such as those prescribed by HIPAA.[7] In the event non-PII compiles into PII, the information system will require re-examination and possible adjustment to the PII confidentiality impact level for that system, possibly invoking use of the Privacy Overlays and other applicable privacy requirements.

(iii) Non-PII becomes PII when combined with a unique identifier or when combined with data elements that have aggregated to become PII

When information that is not otherwise attributed to one individual is associated with PII, then the non-attributable information becomes PII by association. For example, information contained in a financial record of an unidentified individual is not PII, e.g., purchasing history without any other identifying information. However, if the financial record subsequently is linked or linkable to a name or other unique identifier for a particular individual, e.g., credit card number or account number, then the entire financial record becomes PII, i.e., the buying habits of an individual.

Potential Impact Value	Type of adverse effect on organizational operations, organizational assets, or individuals	Expected adverse effect of the loss of confidentiality, integrity, or availability on organizational operations, organizational assets, or individuals
LOW	Limited	(i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; result in minor damage to organizational assets; (ii) result in minor financial loss; or (iii) result in minor harm to individuals.
MODERATE	Serious	(i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
HIGH	Severe or catastrophic	(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Table 2 provides six factors described in NIST SP 800-122, with illustrative examples aligned to the three PII confidentiality impact levels.

Table 2: Illustrative Examples of the Six Factors Described in NIST SP 800-122 as Used in Determining PII Confidentiality Impact Levels[10]

NIST SP 800122 Factors	NIST SP 800-122 PII Confidentiality Impact Level[11]		
	Low	**Moderate**	**High**
Identifiability	Data elements are not directly identifiable alone but may indirectly identify individuals or significantly narrow large datasets.	Combined data elements uniquely and directly identify individuals.	Individual data elements directly identifying unique individuals.
Quantity of PII	A limited number of individuals affected by a loss, theft, or compromise. Limited collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.	A serious or substantial number of individuals affected by loss, theft, or compromise. Serious collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. Aggregation of a serious or substantial amount of data.	A severe or catastrophic number of individuals affected by loss, theft, or compromise. Severe or catastrophic collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. Aggregation of a significantly large amount of data, e.g., "Big Data."
Data Field Sensitivity	Data fields, alone or in combination, have little relevance outside the context.	Data fields, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.	Data fields, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
Obligation to Protect Confidentiality	Government-wide privacy laws, regulations or mandates apply. Violations may result in limited civil penalties.	Role-specific privacy laws, regulations, or mandates (e.g., those that cover certain types of healthcare or financial information) apply that add more restrictive requirements to government-wide	Organization or Mission specific privacy laws, regulations, mandates, or organizational policy apply that add more restrictive requirements to governmentwide or industry-specific

Company and the Internal Revenue Service (IRS), are subject to specific legal obligations to protect certain types of PII." NIST 800-122, Section 3.2.5, advises that "Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with an organization 's legal counsel and privacy officer because relevant laws, regulations, and other mandates are often complex and change over time."

NIST SP 800122 Factors	NIST SP 800-122 PII Confidentiality Impact Level		
	Low	Moderate	High
		requirements. Violations may result in serious civil or criminal penalties.	requirements. Violations may result in severe civil or criminal penalties.
Access to and Location of PII	Located on computers and other devices on an internal network. Access limited to a small population of the organization's workforce, such as a program or office which owns the information on behalf of the organization. Access only allowed at physical locations owned by the organization (e.g., official offices). Backups are stored at government-owned facilities. PII is not stored or transported off-site by employees or contractors.	Located on computers and other devices on a network controlled by the organization. Access limited to a multiple populations of the organization's workforce beyond the direct program or office that owns the information on behalf of the organization. Access only allowed by organization owned equipment outside of the physical locations owned by the organization only with a secured connection (e.g., virtual private network (VPN)). Backups are stored at contractor-owned facilities.	Located on computers and other devices on a network not controlled by the organization or on mobile devices or storage media. Access open to the organization's entire workforce. Remote access allowed by equipment owned by others (e.g., personal mobile devices). Information can be stored on equipment owned by others (e.g., personal USB drive).
Context of Use	Disclosure of the act of collecting, and using the PII, *or* the PII itself is unlikely to result in limited harm to the individual or organization such as name, address, and phone numbers of a list of people who subscribe to a general-interest newsletter.	Disclosure of the act of collecting, and using the PII, *or* the PII itself may result in serious harm to the individual or organization such as name, address, and phone numbers of a list of people who have filed for retirement benefits.	Disclosure of the act of collecting, and using the PII, *or* the PII itself is likely to result in severe or catastrophic harm to the individual or organization such as name, address, and phone numbers of a list of people who work undercover in law enforcement.

Appendix C –Control Allocation Table

Control Types

a. **Common:** Single implementation leveraged and used uniformly across the Company.
b. **Hybrid:** Implementation is split between two or more elements of the Company.
c. **System:** Implementation is unique to the specific system.

ID	Privacy Controls	Identified Control
AP	**Authority and Purpose**	**Control Type**
AP-1	Authority to Collect	**SYSTEM –** **System/Program Level** –PIA, and PA Statement
AP-2	Purpose Specification	**SYSTEM –** **System/Program Level** –PIA, and PA Statement
AR	**Accountability, Audit, and Risk Management**	
AR-1	Governance and Privacy Program	**COMMON –** **Privacy Policy**
AR-2	Privacy Impact and Risk Assessment	**SYSTEM –** **System/Program Level** –PTA/PIA, and PA Statement
AR-3	Privacy Requirements for Contractors and Service Providers	**HYBRID –** **DEPT Level** – Homegrown Canna VA Privacy Program Plan **System/Program Level** – Contract Privacy Provisions
AR-4	Privacy Monitoring and Auditing	**HYBRID –** **DEPT Level** – Homegrown Canna VA DLP Policy **System/Program Level** – DLP and Privacy Monitoring Tools/ Capabilities
AR-5	Privacy Awareness and Training	**HYBRID –** **DEPT Level** – Homegrown Canna VA Privacy Training/ Awareness **System/Program Level** – Company/ System Privacy Training/ Awareness
AR-6	Privacy Reporting	**COMMON –** **DEPT Level** – Homegrown Canna VA PA, PII, BII Breach Notification Plan

ID	Privacy Controls	Identified Control
AR-7	Privacy-Enhanced System Design and Development	**SYSTEM –** **System/Program Level** –PIA, and PA Statement
AR-8	Accounting of Disclosures	**SYSTEM –** **System/Program Level** –PIA, and PA Statement
DI	**Data Quality and Integrity**	
DI-1	Data Quality – Hybrid	**SYSTEM –** **System/Program Level** –PIA, and PA Statement

ID	Privacy Controls	Identified Control
DI-2	Data Integrity and Data Integrity Board	**SYSTEM –** **System/Program Level** – PIA, and PA Statement
DM	**Data Minimization and Retention**	
DM-1	Minimization of Personally Identifiable Information	**SYSTEM –** **System/Program Level** – PIA, and PA Statement
DM-2	Data Retention and Disposal	**SYSTEM –** **System/Program Level** – PIA, and PA Statement, Record Schedule
DM-3	Minimization of PII Used in Testing, Training, and Research	**HYBRID –** **DEPT Level** – Homegrown Canna VA Privacy Program Plan **System/Program Level** – PIA
IP	**Individual Participation and Redress**	
IP-1	Consent	**SYSTEM –** **System/ Program Level** – PIA, and PA Statement
IP-2	Individual Access	**HYBRID –** **DEPT Level** – PIA
IP-3	Redress – System level, unless decision made to determine process at enterprise level, then hybrid	**HYBRID –** **DEPT Level** – Homegrown Canna VA Privacy Program Plan **System/Program Level** – PIA, and PA Statement

ID	Privacy Controls	Identified Control
IP-4	Complaint Management	**HYBRID –** **DEPT Level** – Homegrown Canna VA Privacy Program Plan **System/Program Level** – PIA, and PA Statement
SE	**Security**	
SE-1	Inventory of Personally Identifiable Information	**HYBRID –** **DEPT Level** –Guidance and Reporting **System/Program Level** – PIA, and PA Statement
SE-2	Privacy Incident Response	**HYBRID–** **DEPT Level** – Homegrown Canna VA PII, and BII Breach Notification Plan **System/ Program Level** - Breach Response Processes
TR	**Transparency**	
TR-1	Privacy Notice	**SYSTEM –** **System/Program Level** – PIA, and PA Statement
TR-2	System of Records Notices and Privacy Act Statements	**SYSTEM –** **System/Program Level** – SORN, PIA, and PA Statement

ID	Privacy Controls	Identified Control
TR-3	Dissemination of Privacy Program Information	**COMMON –** **DEPT Level** – Homegrown Canna VA Privacy Program Plan
UL	**Use Limitation**	
UL-1	Internal Use	**SYSTEM –** **System/Program Level** – PIA, and PA Statement
UL-2	Information Sharing with Third Parties	**SYSTEM –** **System/Program Level** – PIA, and PA Statement

Appendix D– Implementing Privacy Overlays

Introduction

This document is comprised of four Privacy Overlays that identify security and privacy control specifications required to protect personally identifiable information (PII), in

Homegrown Canna VA systems and reduce privacy risks to individuals throughout the information lifecycle. The Privacy Overlays support implementation of but are not intended to, and do not, supersede privacy requirements of statute, regulation, or Office of Management and Budget (OMB) policy.

Since the Privacy Act of 1974 established the requirement for "appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records" and "to protect… the integrity" of systems, both the technology and threats thereto have evolved and organizations have had to change the way they protect their information. The National Institute of Standards and Technology (NIST) Special Publication provides the underlying controls necessary to protect PII processing.

systems within Homegrown Canna VA. Based on the Fair Information Practice Principles (FIPPs) and federal privacy requirements, these Privacy Overlays provide a consistent approach for ensuring implementation of "appropriate administrative, technical, and physical safeguards" to protect PII in information systems

irrespective of whether the PII is maintained as part of a system of records. The Privacy Overlays provide a method within existing NIST structures to implement the security and privacy controls necessary to protect PII in today's technology-dependent world.

All PII is not equally sensitive and therefore all PII does not require equal protection. PII with higher sensitivity requires more stringent protections, while PII with lower sensitivity requires less stringent protections. There are three overlays that address the varying sensitivity of PII; Low, Moderate, and High. PHI is a subset of PII and in addition to sensitivity considerations, PHI requires a minimum set of protections that are based on the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Rules. Therefore, PHI is addressed under a fourth overlay, which is applied on top of the Privacy Overlay determined by the sensitivity of the PHI, i.e., Low, Moderate, or High.

Overlays Summary

The table contains a summary of the security and privacy control specifications as they apply in the Privacy Overlays. The detailed specifications and tailoring considerations for each control can be found in the sections that follow. The symbols used in the table are as follows:

- An X sign ("X") indicates the control should be selected.

Table: Privacy Overlays Security and Privacy Controls

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
5.2	AC-1	X	X	X	X	X	X	X	X	X	X
5.3	AC-1	X	X	X	X	X	X	X	X	X	X
7.5.1	AC-1	X	X	X	X	X	X	X	X	X	X
7.5.2	AC-1	X	X	X	X	X	X	X	X	X	X
7.5.3	AC-1	X	X	X	X	X	X	X	X	X	X
A.5.1	AC-1	X	X	X	X	X	X	X	X	X	X
A.5.2	AC-1	X	X	X	X	X	X	X	X	X	X
A.5.4	AC-1	X	X	X	X	X	X	X	X	X	X
A.5.15	AC-1	X	X	X	X	X	X	X	X	X	X
A.5.31	AC-1	X	X	X	X	X	X	X	X	X	X
A.5.36	AC-1	X	X	X	X	X	X	X	X	X	X
A.5.37	AC-1	X	X	X	X	X	X	X	X	X	X
A.8.5	AC-8	X	X	X	X	X	X	X			
5.2	AT-1	X	X	X	X	X	X	X	X	X	X
5.3	AT-1	X	X	X	X	X	X	X	X	X	X
7.5.1	AT-1	X	X	X	X	X	X	X	X	X	X
7.5.2	AT-1	X	X	X	X	X	X	X	X	X	X
7.5.3	AT-1	X	X	X	X	X	X	X	X	X	X
A.5.1	AT-1	X	X	X	X	X	X	X	X	X	X
A.5.2	AT-1	X	X	X	X	X	X	X	X	X	X
A.5.4	AT-1	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
A.5.15	AT-1	X	X	X	X	X	X	X	X	X	X
A.5.31	AT-1	X	X	X	X	X	X	X	X	X	X
A.5.36	AT-1	X	X	X	X	X	X	X	X	X	X
A.5.37	AT-1	X	X	X	X	X	X	X	X	X	X
7.3	AT-2	X	X	X	X	X	X	X	X	X	X
A.6.3	AT-2	X	X	X	X	X	X	X	X	X	X
A.8.7	AT-2	X	X	X	X	X	X	X	X	X	X
A.6.3	AT-3	X	X	X	X	X	X	X	X	X	X
5.2	AU-1	X	X	X	X	X	X	X	X	X	X
5.3	AU-1	X	X	X	X	X	X	X	X	X	X
7.5.1	AU-1	X	X	X	X	X	X	X	X	X	X
7.5.2	AU-1	X	X	X	X	X	X	X	X	X	X
7.5.3	AU-1	X	X	X	X	X	X	X	X	X	X
A.5.1	AU-1	X	X	X	X	X	X	X	X	X	X
A.5.2	AU-1	X	X	X	X	X	X	X	X	X	X
A.5.4	AU-1	X	X	X	X	X	X	X	X	X	X
A.5.15	AU-1	X	X	X	X	X	X	X	X	X	X
A.5.31	AU-1	X	X	X	X	X	X	X	X	X	X
A.5.36	AU-1	X	X	X	X	X	X	X	X	X	X
A.5.37	AU-1	X	X	X	X	X	X	X	X	X	X
A.8.15	AU-2	X	X	X	X	X	X	X			
A.5.28	AU-11	X							X	X	X
A.8.15	AU-11	X							X	X	X
A.8.15	AU-12	X	X	X	X	X	X	X			
5.2	CA-1	X	X	X	X	X	X	X	X	X	X
5.3	CA-1	X	X	X	X	X	X	X	X	X	X
7.5.1	CA-1	X	X	X	X	X	X	X	X	X	X
7.5.2	CA-1	X	X	X	X	X	X	X	X	X	X
7.5.3	CA-1	X	X	X	X	X	X	X	X	X	X
A.5.1	CA-1	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
A.5.2	CA-1	X	X	X	X	X	X	X	X	X	X
A.5.4	CA-1	X	X	X	X	X	X	X	X	X	X
A.5.15	CA-1	X	X	X	X	X	X	X	X	X	X
A.5.31	CA-1	X	X	X	X	X	X	X	X	X	X
A.5.36	CA-1	X	X	X	X	X	X	X	X	X	X
A.5.37	CA-1	X	X	X	X	X	X	X	X	X	X
9.2.1	CA-2	X	X	X	X	X	X	X	X	X	X
9.2.2	CA-2	X	X	X	X	X	X	X	X	X	X
A.5.30	CA-2	X	X	X	X	X	X	X	X	X	X
A.5.36	CA-2	X	X	X	X	X	X	X	X	X	X
A.8.29	CA-2	X	X	X	X	X	X	X	X	X	X
8.3	CA-5	X	X	X	X	X	X	X	X	X	X
9.3.3	CA-5	X	X	X	X	X	X	X	X	X	X
10.2	CA-5	X	X	X	X	X	X	X	X	X	X
9.3.1	CA-6	X	X	X	X	X	X	X	X	X	X
9.3.3	CA-6	X	X	X	X	X	X	X	X	X	X
9.1	CA-7	X	X	X	X	X	X	X	X	X	X
9.3.2	CA-7	X	X	X	X	X	X	X	X	X	X
9.3.3	CA-7	X	X	X	X	X	X	X	X	X	X
A.5.36	CA-7	X	X	X	X	X	X	X	X	X	X
5.2	CM-1	X	X	X	X	X	X	X			
5.3	CM-1	X	X	X	X	X	X	X			
7.5.1	CM-1	X	X	X	X	X	X	X			
7.5.2	CM-1	X	X	X	X	X	X	X			
7.5.3	CM-1	X	X	X	X	X	X	X			
A.5.1	CM-1	X	X	X	X	X	X	X			
A.5.2	CM-1	X	X	X	X	X	X	X			
A.5.4	CM-1	X	X	X	X	X	X	X			
A.5.31	CM-1	X	X	X	X	X	X	X			
A.5.36	CM-1	X	X	X	X	X	X	X			
A.5.37	CM-1	X	X	X	X	X	X	X			

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
A.8.9	CM-1	X	X	X	X	X	X	X			
A.8.9	CM-4	X				X	X	X			
5.2	CP-1	X	X	X	X	X	X	X	X	X	X
5.3	CP-1	X	X	X	X	X	X	X	X	X	X
7.5.1	CP-1	X	X	X	X	X	X	X	X	X	X
7.5.2	CP-1	X	X	X	X	X	X	X	X	X	X
7.5.3	CP-1	X	X	X	X	X	X	X	X	X	X
A.5.1	CP-1	X	X	X	X	X	X	X	X	X	X
A.5.2	CP-1	X	X	X	X	X	X	X	X	X	X
A.5.4	CP-1	X	X	X	X	X	X	X	X	X	X
A.5.31	CP-1	X	X	X	X	X	X	X	X	X	X
A.5.36	CP-1	X	X	X	X	X	X	X	X	X	X
A.5.37	CP-1	X	X	X	X	X	X	X	X	X	X
5.2	IA-1	X	X	X	X	X	X	X			
5.3	IA-1	X	X	X	X	X	X	X			
7.5.1	IA-1	X	X	X	X	X	X	X			
7.5.2	IA-1	X	X	X	X	X	X	X			
7.5.3	IA-1	X	X	X	X	X	X	X			
A.5.1	IA-1	X	X	X	X	X	X	X			
A.5.2	IA-1	X	X	X	X	X	X	X			
A.5.4	IA-1	X	X	X	X	X	X	X			
A.5.31	IA-1	X	X	X	X	X	X	X			
A.5.36	IA-1	X	X	X	X	X	X	X			
A.5.37	IA-1	X	X	X	X	X	X	X			
5.2	IR-1	X	X	X	X	X	X	X	X	X	X
5.3	IR-1	X	X	X	X	X	X	X	X	X	X
7.5.1	IR-1	X	X	X	X	X	X	X	X	X	X
7.5.2	IR-1	X	X	X	X	X	X	X	X	X	X
7.5.3	IR-1	X	X	X	X	X	X	X	X	X	X
A.5.1	IR-1	X	X	X	X	X	X	X	X	X	X
A.5.2	IR-1	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
A.5.4	IR-1	X	X	X	X	X	X	X	X	X	X
A.5.31	IR-1	X	X	X	X	X	X	X	X	X	X
A.5.36	IR-1	X	X	X	X	X	X	X	X	X	X
A.5.37	IR-1	X	X	X	X	X	X	X	X	X	X
A.6.3	IR-2	X	X	X	X	X	X	X	X	X	X
A.5.25	IR-4	X	X	X	X	X	X	X	X	X	X
A.5.26	IR-4	X	X	X	X	X	X	X	X	X	X
A.5.27	IR-4	X	X	X	X	X	X	X	X	X	X
A.5.5	IR-6	X	X	X	X	X	X	X	X	X	X
A.6.8	IR-6	X	X	X	X	X	X	X	X	X	X
7.5.1	IR-8	X	X	X	X	X	X	X	X	X	X
7.5.2	IR-8	X	X	X	X	X	X	X	X	X	X
7.5.3	IR-8	X	X	X	X	X	X	X	X	X	X
A.5.24	IR-8	X	X	X	X	X	X	X	X	X	X
5.2	MP-1	X	X	X	X	X	X	X			
5.3	MP-1	X	X	X	X	X	X	X			
7.5.1	MP-1	X	X	X	X	X	X	X			
7.5.2	MP-1	X	X	X	X	X	X	X			
7.5.3	MP-1	X	X	X	X	X	X	X			
A.5.1	MP-1	X	X	X	X	X	X	X			
A.5.2	MP-1	X	X	X	X	X	X	X			
A.5.4	MP-1	X	X	X	X	X	X	X			
A.5.31	MP-1	X	X	X	X	X	X	X			
A.5.36	MP-1	X	X	X	X	X	X	X			
A.5.37	MP-1	X	X	X	X	X	X	X			
A.5.10	MP-6	X	X	X	X						
A.7.10	MP-6	X	X	X	X						
A.7.14	MP-6	X	X	X	X						
A.8.10	MP-6	X	X	X	X						
5.2	PE-1	X	X	X	X	X	X	X	X	X	X
5.3	PE-1	X	X	X	X	X	X	X	X	X	X
7.5.1	PE-1	X	X	X	X	X	X	X	X	X	X
7.5.2	PE-1	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
7.5.3	PE-1	X	X	X	X	X	X	X	X	X	X
A.5.1	PE-1	X	X	X	X	X	X	X	X	X	X
A.5.2	PE-1	X	X	X	X	X	X	X	X	X	X
A.5.4	PE-1	X	X	X	X	X	X	X	X	X	X
A.5.31	PE-1	X	X	X	X	X	X	X	X	X	X
A.5.36	PE-1	X	X	X	X	X	X	X	X	X	X
A.5.37	PE-1	X	X	X	X	X	X	X	X	X	X
A.7.2	PE-2	X	X	X	X	X	X	X	X	X	X
5.2	PL-1	X	X	X	X	X	X	X	X	X	X
5.3	PL-1	X	X	X	X	X	X	X	X	X	X
7.5.1	PL-1	X	X	X	X	X	X	X	X	X	X
7.5.2	PL-1	X	X	X	X	X	X	X	X	X	X
7.5.3	PL-1	X	X	X	X	X	X	X	X	X	X
A.5.1	PL-1	X	X	X	X	X	X	X	X	X	X
A.5.2	PL-1	X	X	X	X	X	X	X	X	X	X
A.5.4	PL-1	X	X	X	X	X	X	X	X	X	X
A.5.31	PL-1	X	X	X	X	X	X	X	X	X	X
A.5.36	PL-1	X	X	X	X	X	X	X	X	X	X
A.5.37	PL-1	X	X	X	X	X	X	X	X	X	X
7.5.1	PL-2	X	X	X	X	X	X	X	X	X	X
7.5.2	PL-2	X	X	X	X	X	X	X	X	X	X
7.5.3	PL-2	X	X	X	X	X	X	X	X	X	X
10.2	PL-2	X	X	X	X	X	X	X	X	X	X
A.5.8	PL-2	X	X	X	X	X	X	X	X	X	X
A.5.4	PL-4	X	X	X	X	X	X	X	X	X	X
A.5.10	PL-4	X	X	X	X	X	X	X	X	X	X
A.6.2	PL-4	X	X	X	X	X	X	X	X	X	X
4.1	PM-1	X	X	X	X	X	X	X	X	X	X
4.2	PM-1	X	X	X	X	X	X	X	X	X	X
4.3	PM-1	X	X	X	X	X	X	X	X	X	X
4.4	PM-1	X	X	X	X	X	X	X	X	X	X
5.2	PM-1	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
5.3	PM-1	X	X	X	X	X	X	X	X	X	X
6.1.1	PM-1	X	X	X	X	X	X	X	X	X	X
6.2	PM-1	X	X	X	X	X	X	X	X	X	X
7.4	PM-1	X	X	X	X	X	X	X	X	X	X
7.5.1	PM-1	X	X	X	X	X	X	X	X	X	X
7.5.2	PM-1	X	X	X	X	X	X	X	X	X	X
7.5.3	PM-1	X	X	X	X	X	X	X	X	X	X
8.1	PM-1	X	X	X	X	X	X	X	X	X	X
9.3.1	PM-1	X	X	X	X	X	X	X	X	X	X
10.1	PM-1	X	X	X	X	X	X	X	X	X	X
A.5.1	PM-1	X	X	X	X	X	X	X	X	X	X
A.5.2	PM-1	X	X	X	X	X	X	X	X	X	X
A.5.4	PM-1	X	X	X	X	X	X	X	X	X	X
A.5.31	PM-1	X	X	X	X	X	X	X	X	X	X
A.5.36	PM-1	X	X	X	X	X	X	X	X	X	X
5.1	PM-3	X	X	X	X	X	X	X	X	X	X
6.2	PM-3	X	X	X	X	X	X	X	X	X	X
7.1	PM-3	X	X	X	X	X	X	X	X	X	X
6.1.1	PM-4	X	X	X	X	X	X	X	X	X	X
6.2	PM-4	X	X	X	X	X	X	X	X	X	X
7.5.1	PM-4	X	X	X	X	X	X	X	X	X	X
7.5.2	PM-4	X	X	X	X	X	X	X	X	X	X
7.5.3	PM-4	X	X	X	X	X	X	X	X	X	X
8.3	PM-4	X	X	X	X	X	X	X	X	X	X
9.3.2	PM-4	X	X	X	X	X	X	X	X	X	X
10.2	PM-4	X	X	X	X	X	X	X	X	X	X
5.3	PM-6	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
6.1.1	PM-6	X	X	X	X	X	X	X	X	X	X
6.2	PM-6	X	X	X	X	X	X	X	X	X	X
9.1	PM-6	X	X	X	X	X	X	X	X	X	X
4.3	PM-9	X	X	X	X	X	X	X	X	X	X
4.4	PM-9	X	X	X	X	X	X	X	X	X	X
6.1.1	PM-9	X	X	X	X	X	X	X	X	X	X
6.1.2	PM-9	X	X	X	X	X	X	X	X	X	X
6.2	PM-9	X	X	X	X	X	X	X	X	X	X
7.5.1	PM-9	X	X	X	X	X	X	X	X	X	X
7.5.2	PM-9	X	X	X	X	X	X	X	X	X	X
7.5.3	PM-9	X	X	X	X	X	X	X	X	X	X
10.1	PM-9	X	X	X	X	X	X	X	X	X	X
A.5.2	PM-10	X	X	X	X	X	X	X	X	X	X
4.1	PM-11	X	X	X	X	X	X	X	X	X	X
7.2	PM-13	X	X	X	X	X	X	X	X	X	X
A.6.3	PM-13	X	X	X	X	X	X	X	X	X	X
6.2	PM-14	X	X	X	X	X	X	X	X	X	X
A.5.4	PM-18	X	X	X	X	X	X	X	X	X	X
4.3	PM-28	X	X	X	X	X	X	X	X	X	X
6.1.2	PM-28	X	X	X	X	X	X	X	X	X	X
6.2	PM-28	X	X	X	X	X	X	X	X	X	X
7.4	PM-28	X	X	X	X	X	X	X	X	X	X
7.5.1	PM-28	X	X	X	X	X	X	X	X	X	X
7.5.2	PM-28	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
7.5.3	PM-28	X	X	X	X	X	X	X	X	X	X
5.1	PM-29	X	X	X	X	X	X	X	X	X	X
5.3	PM-29	X	X	X	X	X	X	X	X	X	X
9.3.1	PM-29	X	X	X	X	X	X	X	X	X	X
A.5.2	PM-29	X	X	X	X	X	X	X	X	X	X
4.4	PM-30	X	X	X	X	X	X	X	X	X	X
6.2	PM-30	X	X	X	X	X	X	X	X	X	X
7.5.1	PM-30	X	X	X	X	X	X	X	X	X	X
7.5.2	PM-30	X	X	X	X	X	X	X	X	X	X
7.5.3	PM-30	X	X	X	X	X	X	X	X	X	X
10.2	PM-30	X	X	X	X	X	X	X	X	X	X
4.4	PM-31	X	X	X	X	X	X	X	X	X	X
6.2	PM-31	X	X	X	X	X	X	X	X	X	X
7.4	PM-31	X	X	X	X	X	X	X	X	X	X
7.5.1	PM-31	X	X	X	X	X	X	X	X	X	X
7.5.2	PM-31	X	X	X	X	X	X	X	X	X	X
7.5.3	PM-31	X	X	X	X	X	X	X	X	X	X
9.1	PM-31	X	X	X	X	X	X	X	X	X	X
9.2.2	PM-31	X	X	X	X	X	X	X	X	X	X
10.1	PM-31	X	X	X	X	X	X	X	X	X	X
10.2	PM-31	X	X	X	X	X	X	X	X	X	X
5.2	PS-1	X	X	X	X	X	X	X	X	X	X
5.3	PS-1	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
7.5.1	PS-1	X	X	X	X	X	X	X	X	X	X
7.5.2	PS-1	X	X	X	X	X	X	X	X	X	X
7.5.3	PS-1	X	X	X	X	X	X	X	X	X	X
A.5.1	PS-1	X	X	X	X	X	X	X	X	X	X
A.5.2	PS-1	X	X	X	X	X	X	X	X	X	X
A.5.4	PS-1	X	X	X	X	X	X	X	X	X	X
A.5.31	PS-1	X	X	X	X	X	X	X	X	X	X
A.5.36	PS-1	X	X	X	X	X	X	X	X	X	X
A.5.37	PS-1	X	X	X	X	X	X	X	X	X	X
A.6.1	PS-3	X	X	X	X	X	X				
A.5.4	PS-6	X	X	X	X	X	X	X			
A.6.2	PS-6	X	X	X	X	X	X	X			
A.6.6	PS-6	X	X	X	X	X	X	X			
7.3	PS-8	X	X	X	X	X	X	X	X	X	X
A.6.4	PS-8	X	X	X	X	X	X	X	X	X	X
A.5.2	PS-9	X	X	X	X	X	X	X	X	X	X
A.5.4	PT-1	X	X	X	X	X	X	X	X	X	X
5.2	RA-1	X	X	X	X	X	X	X	X	X	X
5.3	RA-1	X	X	X	X	X	X	X	X	X	X
7.5.1	RA-1	X	X	X	X	X	X	X	X	X	X
7.5.2	RA-1	X	X	X	X	X	X	X	X	X	X
7.5.3	RA-1	X	X	X	X	X	X	X	X	X	X
A.5.1	RA-1	X	X	X	X	X	X	X	X	X	X
A.5.2	RA-1	X	X	X	X	X	X	X	X	X	X
A.5.4	RA-1	X	X	X	X	X	X	X	X	X	X
A.5.31	RA-1	X	X	X	X	X	X	X	X	X	X
A.5.36	RA-1	X	X	X	X	X	X	X	X	X	X
A.5.37	RA-1	X	X	X	X	X	X	X	X	X	X
A.5.12	RA-2	X	X	X	X	X	X	X	X	X	X
6.1.2	RA-3	X	X	X	X	X	X	X	X	X	X
8.2	RA-3	X	X	X	X	X	X	X	X	X	X
9.3.2	RA-3	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
A.8.8	RA-3	X	X	X	X	X	X	X	X	X	X
6.1.3	RA-7	X	X	X	X	X	X	X	X	X	X
8.3	RA-7	X	X	X	X	X	X	X	X	X	X
10.2	RA-7	X	X	X	X	X	X	X	X	X	X
5.2	SA-1	X	X	X	X	X	X	X	X	X	X
5.3	SA-1	X	X	X	X	X	X	X	X	X	X
7.5.1	SA-1	X	X	X	X	X	X	X	X	X	X
7.5.2	SA-1	X	X	X	X	X	X	X	X	X	X
7.5.3	SA-1	X	X	X	X	X	X	X	X	X	X
8.1	SA-1	X	X	X	X	X	X	X	X	X	X
A.5.1	SA-1	X	X	X	X	X	X	X	X	X	X
A.5.2	SA-1	X	X	X	X	X	X	X	X	X	X
A.5.4	SA-1	X	X	X	X	X	X	X	X	X	X
A.5.23	SA-1	X	X	X	X	X	X	X	X	X	X
A.5.31	SA-1	X	X	X	X	X	X	X	X	X	X
A.5.36	SA-1	X	X	X	X	X	X	X	X	X	X
A.5.37	SA-1	X	X	X	X	X	X	X	X	X	X
A.5.2	SA-3	X	X	X	X	X	X	X	X	X	X
A.5.8	SA-3	X	X	X	X	X	X	X	X	X	X
A.8.25	SA-3	X	X	X	X	X	X	X	X	X	X
A.8.31	SA-3	X	X	X	X	X	X	X	X	X	X
8.1	SA-4	X	X	X	X	X	X	X	X	X	X
A.5.8	SA-4	X	X	X	X	X	X	X	X	X	X
A.5.20	SA-4	X	X	X	X	X	X	X	X	X	X
A.5.23	SA-4	X	X	X	X	X	X	X	X	X	X
A.8.29	SA-4	X	X	X	X	X	X	X	X	X	X
A.8.30	SA-4	X	X	X	X	X	X	X	X	X	X
A.5.2	SA-9	X	X	X	X	X	X	X	X	X	X
A.5.4	SA-9	X	X	X	X	X	X	X	X	X	X
A.5.8	SA-9	X	X	X	X	X	X	X	X	X	X
A.5.14	SA-9	X	X	X	X	X	X	X	X	X	X
A.5.22	SA-9	X	X	X	X	X	X	X	X	X	X
A.5.23	SA-9	X	X	X	X	X	X	X	X	X	X
A.8.21	SA-9	X	X	X	X	X	X	X	X	X	X
A.8.29	SA-11	X		X	X		X	X		X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
A.8.30	SA-11	X		X	X		X	X		X	X
5.2	SC-1	X	X	X	X	X	X	X	X	X	X
5.3	SC-1	X	X	X	X	X	X	X	X	X	X
7.5.1	SC-1	X	X	X	X	X	X	X	X	X	X
7.5.2	SC-1	X	X	X	X	X	X	X	X	X	X
7.5.3	SC-1	X	X	X	X	X	X	X	X	X	X
A.5.1	SC-1	X	X	X	X	X	X	X	X	X	X
A.5.2	SC-1	X	X	X	X	X	X	X	X	X	X
A.5.4	SC-1	X	X	X	X	X	X	X	X	X	X
A.5.31	SC-1	X	X	X	X	X	X	X	X	X	X
A.5.36	SC-1	X	X	X	X	X	X	X	X	X	X
A.5.37	SC-1	X	X	X	X	X	X	X	X	X	X
5.2	SI-1	X	X	X	X	X	X	X	X	X	X
5.3	SI-1	X	X	X	X	X	X	X	X	X	X
7.5.1	SI-1	X	X	X	X	X	X	X	X	X	X
7.5.2	SI-1	X	X	X	X	X	X	X	X	X	X
7.5.3	SI-1	X	X	X	X	X	X	X	X	X	X
A.5.1	SI-1	X	X	X	X	X	X	X	X	X	X
A.5.2	SI-1	X	X	X	X	X	X	X	X	X	X
A.5.4	SI-1	X	X	X	X	X	X	X	X	X	X
A.5.31	SI-1	X	X	X	X	X	X	X	X	X	X
A.5.36	SI-1	X	X	X	X	X	X	X	X	X	X
A.5.37	SI-1	X	X	X	X	X	X	X	X	X	X
5.2	SR-1	X	X	X	X	X	X	X	X	X	X
5.3	SR-1	X	X	X	X	X	X	X	X	X	X
7.5.1	SR-1	X	X	X	X	X	X	X	X	X	X
7.5.2	SR-1	X	X	X	X	X	X	X	X	X	X
7.5.3	SR-1	X	X	X	X	X	X	X	X	X	X
A.5.1	SR-1	X	X	X	X	X	X	X	X	X	X
A.5.2	SR-1	X	X	X	X	X	X	X	X	X	X
A.5.4	SR-1	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
A.5.19	SR-1	X	X	X	X	X	X	X	X	X	X
A.5.31	SR-1	X	X	X	X	X	X	X	X	X	X
A.5.36	SR-1	X	X	X	X	X	X	X	X	X	X
A.5.37	SR-1	X	X	X	X	X	X	X	X	X	X
9.1	CA-1	X	X	X	X	X	X	X	X	X	X
9.2.1	CA-7	X	X	X	X	X	X	X	X	X	X
9.2.2	CA-1	X	X	X	X	X	X	X	X	X	X
9.3.1	CA-1	X	X	X	X	X	X	X	X	X	X
9.3.2	CA-7(4)	X	X	X	X	X	X	X	X	X	X
10.1	PM-30	X	X	X	X	X	X	X	X	X	X
5.1	AC-1	X	X	X	X	X	X	X	X	X	X
5.1	AT-1	X	X	X	X	X	X	X	X	X	X
5.1	AU-1	X	X	X	X	X	X	X	X	X	X
5.1	CA-1	X	X	X	X	X	X	X	X	X	X
5.1	CM-1	X	X	X	X	X	X	X			
5.1	CP-1	X	X	X	X	X	X	X	X	X	X
5.1	IA-1	X	X	X	X	X	X	X			
5.1	IR-1	X	X	X	X	X	X	X	X	X	X
5.1	MP-1	X	X	X	X	X	X	X			
5.1	PE-1	X	X	X	X	X	X	X	X	X	X
5.1	PL-1	X	X	X	X	X	X	X	X	X	X
5.1	PM-1	X	X	X	X	X	X	X	X	X	X
5.1	PS-1	X	X	X	X	X	X	X	X	X	X
5.1	PT-1	X	X	X	X	X	X	X	X	X	X
5.1	RA-1	X	X	X	X	X	X	X	X	X	X
5.1	SA-1	X	X	X	X	X	X	X	X	X	X
5.1	SC-1	X	X	X	X	X	X	X	X	X	X
5.1	SI-1	X	X	X	X	X	X	X	X	X	X
5.1	SR-1	X	X	X	X	X	X	X	X	X	X
5.2	AC-1	X	X	X	X	X	X	X	X	X	X
5.2	AT-1	X	X	X	X	X	X	X	X	X	X
5.2	AU-1	X	X	X	X	X	X	X	X	X	X
5.2	CA-1	X	X	X	X	X	X	X	X	X	X
5.2	CM-1	X	X	X	X	X	X	X			
5.2	CP-1	X	X	X	X	X	X	X	X	X	X
5.2	IA-1	X	X	X	X	X	X	X			
5.2	IR-1	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
5.2	MP-1	X	X	X	X	X	X	X			
5.2	PE-1	X	X	X	X	X	X	X	X	X	X
5.2	PL-1	X	X	X	X	X	X	X	X	X	X
5.2	PM-1	X	X	X	X	X	X	X	X	X	X
5.2	PS-1	X	X	X	X	X	X	X	X	X	X
5.2	PT-1	X	X	X	X	X	X	X	X	X	X
5.2	RA-1	X	X	X	X	X	X	X	X	X	X
5.2	SA-1	X	X	X	X	X	X	X	X	X	X
5.2	SC-1	X	X	X	X	X	X	X	X	X	X
5.2	SI-1	X	X	X	X	X	X	X	X	X	X
5.2	SR-1	X	X	X	X	X	X	X	X	X	X
5.2	PS-1	X	X	X	X	X	X	X	X	X	X
5.2	SA-3	X	X	X	X	X	X	X	X	X	X
5.2	SA-9	X	X	X	X	X	X	X	X	X	X
5.2	PM-10	X	X	X	X	X	X	X	X	X	X
5.4	PM-18	X	X	X	X	X	X	X	X	X	X
5.4	AC-1	X	X	X	X	X	X	X	X	X	X
5.4	AT-1	X	X	X	X	X	X	X	X	X	X
5.4	AU-1	X	X	X	X	X	X	X	X	X	X
5.4	CA-1	X	X	X	X	X	X	X	X	X	X
5.4	CM-1	X	X	X	X	X	X	X			
5.4	CP-1	X	X	X	X	X	X	X	X	X	X
5.4	IA-1	X	X	X	X	X	X	X			
5.4	IR-1	X	X	X	X	X	X	X	X	X	X
5.4	MP-1	X	X	X	X	X	X	X			
5.4	PE-1	X	X	X	X	X	X	X	X	X	X
5.4	PL-1	X	X	X	X	X	X	X	X	X	X
5.4	PM-1	X	X	X	X	X	X	X	X	X	X
5.4	PS-1	X	X	X	X	X	X	X	X	X	X
5.4	PT-1	X	X	X	X	X	X	X	X	X	X
5.4	RA-1	X	X	X	X	X	X	X	X	X	X
5.4	SA-1	X	X	X	X	X	X	X	X	X	X
5.4	SC-1	X	X	X	X	X	X	X	X	X	X
5.4	SI-1	X	X	X	X	X	X	X	X	X	X
5.4	SR-1	X	X	X	X	X	X	X	X	X	X
5.5	IR-6	X	X	X	X	X	X	X	X	X	X
5.8	PL-2	X	X	X	X	X	X	X	X	X	X
5.8	PL-8	X	X	X	X	X	X	X	X	X	X
5.8	SA-3	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
5.8	SA-4	X	X	X	X	X	X	X	X	X	X
5.8	SA-9	X	X	X	X	X	X	X	X	X	X
5.10	MP-6	X	X	X	X						
5.10	PL-4	X	X	X	X	X	X	X	X	X	X
5.12	RA-2	X	X	X	X	X	X	X	X	X	X
5.14	PS-6	X	X	X	X	X	X	X			
5.14	SA-9	X	X	X	X	X	X	X	X	X	X
5.15	AC-1	X	X	X	X	X	X	X	X	X	X
5.19	SR-1	X	X	X	X	X	X	X	X	X	X
5.20	SA-4	X	X	X	X	X	X	X	X	X	X
5.22	SA-9	X	X	X	X	X	X	X	X	X	X
5.23	SA-1	X	X	X	X	X	X	X	X	X	X
5.23	SA-4	X	X	X	X	X	X	X	X	X	X
5.23	SA-9	X	X	X	X	X	X	X	X	X	X
5.24	IR-8	X	X	X	X	X	X	X	X	X	X
5.26	IR-4	X	X	X	X	X	X	X	X	X	X
5.27	IR-4	X	X	X	X	X	X	X	X	X	X
5.28	AU-11	X							X	X	X
5.31	AC-1	X	X	X	X	X	X	X	X	X	X
5.31	AT-1	X	X	X	X	X	X	X	X	X	X
5.31	AU-1	X	X	X	X	X	X	X	X	X	X
5.31	CA-1	X	X	X	X	X	X	X	X	X	X
5.31	CM-1	X	X	X	X	X	X	X			
5.31	CP-1	X	X	X	X	X	X	X	X	X	X
5.31	IA-1	X	X	X	X	X	X	X			
5.31	IR-1	X	X	X	X	X	X	X	X	X	X
5.31	MP-1	X	X	X	X	X	X	X			
5.31	PE-1	X	X	X	X	X	X	X	X	X	X
5.31	PL-1	X	X	X	X	X	X	X	X	X	X
5.31	PM-1	X	X	X	X	X	X	X	X	X	X
5.31	PS-1	X	X	X	X	X	X	X	X	X	X
5.31	PT-1	X	X	X	X	X	X	X	X	X	X
5.31	RA-1	X	X	X	X	X	X	X	X	X	X
5.31	SA-1	X	X	X	X	X	X	X	X	X	X
5.31	SC-1	X	X	X	X	X	X	X	X	X	X
5.31	SI-1	X	X	X	X	X	X	X	X	X	X
5.31	SR-1	X	X	X	X	X	X	X	X	X	X
5.34	PM-18	X	X	X	X	X	X	X	X	X	X
5.34	PT-1	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
5.34	PT-3	X	X	X	X	X	X	X	X	X	X
5.34	PT-7	X	X	X	X	X	X	X	X	X	X
5.34	PL-2	X	X	X	X	X	X	X	X	X	X
5.34	PL-8	X	X	X	X	X	X	X	X	X	X
5.36	AC-1	X	X	X	X	X	X	X	X	X	X
5.36	AT-1	X	X	X	X	X	X	X	X	X	X
5.36	AU-1	X	X	X	X	X	X	X	X	X	X
5.36	CA-1	X	X	X	X	X	X	X	X	X	X
5.36	CM-1	X	X	X	X	X	X	X			
5.36	CP-1	X	X	X	X	X	X	X	X	X	X
5.36	IA-1	X	X	X	X	X	X	X			
5.36	IR-1	X	X	X	X	X	X	X	X	X	X
5.36	MP-1	X	X	X	X	X	X	X			
5.36	PE-1	X	X	X	X	X	X	X	X	X	X
5.36	PL-1	X	X	X	X	X	X	X	X	X	X
5.36	PM-1	X	X	X	X	X	X	X	X	X	X
5.36	PS-1	X	X	X	X	X	X	X	X	X	X
5.36	PT-1	X	X	X	X	X	X	X	X	X	X
5.36	RA-1	X	X	X	X	X	X	X	X	X	X
5.36	SA-1	X	X	X	X	X	X	X	X	X	X
5.36	SC-1	X	X	X	X	X	X	X	X	X	X
5.36	SI-1	X	X	X	X	X	X	X	X	X	X
5.36	SR-1	X	X	X	X	X	X	X	X	X	X
5.37	AC-1	X	X	X	X	X	X	X	X	X	X
5.37	AT-1	X	X	X	X	X	X	X	X	X	X
5.37	AU-1	X	X	X	X	X	X	X	X	X	X
5.37	CA-1	X	X	X	X	X	X	X	X	X	X
5.37	CM-1	X	X	X	X	X	X	X			
5.37	CP-1	X	X	X	X	X	X	X	X	X	X
5.37	IA-1	X	X	X	X	X	X	X			
5.37	IR-1	X	X	X	X	X	X	X	X	X	X
5.37	MP-1	X	X	X	X	X	X	X			
5.37	PE-1	X	X	X	X	X	X	X	X	X	X
5.37	PL-1	X	X	X	X	X	X	X	X	X	X
5.37	PM-1	X	X	X	X	X	X	X	X	X	X
5.37	PS-1	X	X	X	X	X	X	X	X	X	X
5.37	PT-1	X	X	X	X	X	X	X	X	X	X
5.37	RA-1	X	X	X	X	X	X	X	X	X	X
5.37	SA-1	X	X	X	X	X	X	X	X	X	X
5.37	SC-1	X	X	X	X	X	X	X	X	X	X

27001:2022	RMF	Privacy Control Baseline	Confidentiality			Integrity			Availability		
			L	M	H	L	M	H	L	M	H
5.37	SI-1	X	X	X	X	X	X	X	X	X	X
5.37	SR-1	X	X	X	X	X	X	X	X	X	X
6.1	PS-3	X	X	X	X	X	X				
6.2	PL-4	X	X	X	X	X	X	X	X	X	X
6.2	PS-6	X	X	X	X	X	X	X			
6.3	AT-2	X	X	X	X	X	X	X	X	X	X
6.3	AT-3	X	X	X	X	X	X	X	X	X	X
6.3	IR-2	X	X	X	X	X	X	X	X	X	X
6.3	PM-13	X	X	X	X	X	X	X	X	X	X
6.4	PS-8	X	X	X	X	X	X	X	X	X	X
6.6	PS-6	X	X	X	X	X	X	X			
6.8	IR-6	X	X	X	X	X	X	X	X	X	X
7.2	PE-2	X	X	X	X	X	X	X	X	X	X
7.10	MP-6	X	X	X	X						
7.14	MP-6	X	X	X	X						
8.5	AC-8	X	X	X	X	X	X	X			
8.7	AT-2	X	X	X	X	X	X	X	X	X	X
8.8	RA-3	X	X	X	X	X	X	X	X	X	X
8.9	CM-1	X	X	X	X	X	X	X			
8.9	CM-4	X				X	X	X			
8.10	MP-6	X	X	X	X						
8.15	AU-11	X							X	X	X
8.15	AU-12	X	X	X	X	X	X	X			
8.21	SA-9	X	X	X	X	X	X	X	X	X	X
8.25	SA-3	X	X	X	X	X	X	X	X	X	X
8.29	SA-4	X	X	X	X	X	X	X	X	X	X
8.30	SA-4	X	X	X	X	X	X	X	X	X	X
8.31	SA-3	X	X	X	X	X	X	X	X	X	X