Schedule Train CUI certification

V1.0. Current as of January 23, 2024

I certify that ScheduleTrain is compliant with NIST Special Publication 800-171, Revision 2: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations. The sections of this document below each correspond to a section in Publication 800-171, Chapter 3: The Requirements. It is compliant up to IL4.

3.1: Access control-channel

In accordance with Section 3.1 "Access Control" of SP 800-171, Revision 2, ScheduleTrain, utilized by military squadrons and wings and operated on various platforms including squadron scheduling computers, personal computers, and mobile devices, adheres to stringent access control measures.

Requirement 3.1.1 mandates limiting system access to authorized users, processes, and devices. We implement this through a strict permissions hierarchy, where users are granted only the privileges necessary for their role. For instance, most users can only view their squadron's schedule and training plan, while scheduling shop members can edit schedules, and flight commanders and ADOs have additional permissions like approving schedules or leave.

In line with 3.1.2, system access is limited to the types of transactions and functions that authorized users are permitted to execute. This ensures that users can only perform actions that are within their role's scope, thereby enhancing the security and integrity of the system.

Addressing 3.1.3, we control the flow of CUI in accordance with approved authorizations, regulating where and how information can travel within and between systems. This includes implementing boundary protection devices and enforcing information flow control policies.

Requirement 3.1.4 focuses on separating the duties of individuals to reduce the risk of malevolent activity. We divide functions among different individuals or roles, ensuring that no single individual has control over multiple critical functions.

As per 3.1.5, we employ the principle of least privilege, including for specific security functions and privileged accounts. Users and processes are provided with only those privileges which are essential for the performance of their tasks.

Requirement 3.1.6 ensures that non-privileged accounts or roles are used when accessing nonsecurity functions, limiting exposure when operating from within privileged accounts.

In accordance with 3.1.7, we prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. This helps detect and mitigate the misuse of privileged functions.

Requirement 3.1.8 focuses on limiting unsuccessful logon attempts to prevent unauthorized access, while 3.1.9 ensures that privacy and security notices are provided in line with applicable CUI rules.

For 3.1.10, we use session lock with pattern-hiding displays to prevent data access and viewing after a period of inactivity, enhancing data confidentiality.

Addressing 3.1.11, user sessions are automatically terminated after a defined condition, such as a period of inactivity, to further secure system access.

Requirement 3.1.12 involves monitoring and controlling remote access sessions. This is particularly relevant given the operational necessity of ScheduleTrain on various devices, including mobile platforms.

As per 3.1.13, we employ cryptographic mechanisms to protect the confidentiality of remote access sessions, in line with [NIST CRYPTO].

Requirement 3.1.14 focuses on routing remote access via managed access control points to enhance organizational control over such connections.

In accordance with 3.1.15, we authorize remote execution of privileged commands and remote access to security-relevant information, controlling such access to mitigate potential risks.

Requirement 3.1.16 mandates that wireless access be authorized prior to allowing connections, while 3.1.17 ensures the protection of wireless access using authentication and encryption.

Addressing 3.1.18, we control the connection of mobile devices to organizational systems, and per 3.1.19, we encrypt CUI on mobile devices and computing platforms.

In line with 3.1.20, we verify and control connections to and use of external systems, ensuring compliance with organizational security policies.

Requirement 3.1.21 limits the use of portable storage devices on external systems, and 3.1.22 controls CUI posted or processed on publicly accessible systems.

Through these comprehensive access control measures, we ensure that only authorized users can access and perform actions within our system, safeguarding the integrity and confidentiality of CUI and aligning with the operational requirements of our military user base.

3.2: Awareness and training

ScheduleTrain has instituted a comprehensive awareness program for all users, including flight commanders, ADOs, schedulers, and aircrew. Recognizing the importance of educating our personnel on security risks and the policies, standards, and procedures integral to system security, we have integrated a detailed security guide directly accessible from the application's scheduling page. This guide ensures immediate and constant access to crucial information about security practices and procedures, thus fostering continuous awareness. Moreover, the content of this guide and our other awareness materials are tailored to meet the specific needs of the systems our personnel interact with.

In alignment with the guidelines from [SP 800-50], our approach to security awareness extends beyond formal training; we employ varied techniques such as displaying easily-available security guidelines, requiring regular password updates, and deactivating unused user and squadron accounts. These measures ensure that our team is not only aware of the basic requirements of information security but also understands their role in maintaining it and responding to potential security incidents.

Furthermore, adhering to the mandates of Section 3.2.2, ScheduleTrain encourages that all personnel receive training that is specifically aligned with their duties and responsibilities. The training content is designed based on individual roles and the security requirements of our systems, ensuring that each team member, from system developers to network administrators, receives relevant and practical knowledge. This role-based training encompasses a broad spectrum of security aspects, including management, operational, and technical controls. It should also cover policies, procedures, and tools specific to the security roles.

3.3: Audit and accountability

In accordance with Section 3.3, ScheduleTrain has established robust audit and accountability mechanisms. Complying with requirement 3.3.1, our system is engineered to create, retain, and manage comprehensive audit logs and records. Our database retains all this information indefinitely. These logs capture a wide array of system events, including, but not limited to, password changes, failed logon attempts, administrative privilege usage, and unauthorized system activities. The system is designed to log events at various levels of abstraction, from packet-level network data to high-level user actions, allowing for precise monitoring and analysis. This granularity in logging enables us to effectively investigate and report unlawful or unauthorized activities while balancing system performance needs. The audit records include essential information such as timestamps, user/process identifiers, event descriptions, and outcomes, ensuring a thorough understanding of each event.

In response to requirements 3.3.2 to 3.3.9, our system ensures that the actions of individual users are uniquely traceable, maintaining accountability and facilitating the investigation of any security incidents. We regularly review and update our logged events (3.3.3) to ensure relevance and sufficiency in the ever-evolving security landscape. Additionally, our system is equipped to alert in the event of any audit logging process failure (3.3.4), safeguarding against unnoticed compromises in our audit capabilities. To support investigations and responses to suspicious activities, we have implemented procedures for correlating audit record review, analysis, and reporting processes (3.3.5). Our system also features audit record reduction and report generation capabilities (3.3.6), providing analysts with actionable insights and facilitating on-demand reporting. To ensure accuracy and consistency in our audit records, our system's internal clocks are synchronized with an authoritative time source (3.3.7). Furthermore, we rigorously protect our audit information and logging tools from unauthorized access, modification, and deletion (3.3.8), and we strictly limit the management of audit logging functionalities to a subset of privileged users (3.3.9), thereby reducing the risk of internal tampering and ensuring the integrity of our audit processes.

These measures collectively ensure that ScheduleTrain not only complies with the SP 800-171, Revision 2 guidelines but also provides a secure and accountable environment for handling CUI.

3.4: Configuration management

In alignment with Section 3.4, ScheduleTrain adheres to stringent configuration management protocols to ensure the security and integrity of CUI. Complying with requirement 3.4.1, we have established and maintain baseline configurations and inventories. This includes detailed documentation of all hardware, software, firmware, and relevant documentation throughout their development life cycles. Our baseline configurations are routinely reviewed and updated to reflect any changes in the system, in adherence to the established security standards and in response to identified security risks.

To fulfill requirement 3.4.2, we enforce strict security configuration settings for all information technology products used within our systems. These settings are designed to minimize vulnerabilities and are aligned with recognized security benchmarks for each type of technology employed. In accordance with requirements 3.4.3 and 3.4.4, we have implemented robust processes for tracking, reviewing, approving or disapproving, and logging changes to our systems. All changes undergo a thorough security impact analysis prior to implementation to ensure they do not adversely affect the security posture of our systems.

Furthermore, we strictly adhere to the principles of least functionality (3.4.6) and prevent the use of nonessential programs, functions, ports, protocols, and services (3.4.7), thereby reducing the risk of unauthorized access or compromise. Our approach to software execution is governed by a deny-by-exception (blacklisting) policy (3.4.8), ensuring that only authorized software is permitted to run on our systems. Finally, user-installed software is tightly controlled and monitored (3.4.9) to prevent the introduction of unauthorized or potentially harmful applications. These measures collectively ensure that our configuration management practices robustly safeguard the integrity and security of the CUI handled by ScheduleTrain.

3.5: Identification and authentication

In strict compliance with Section 3.5 "Identification and Authentication", ScheduleTrain employs rigorous identification and authentication measures to safeguard CUI. Meeting the criteria of requirement 3.5.1, our system is designed to accurately identify system users, processes acting on behalf of users, and devices, utilizing unique identifiers such as user names, Media Access Control (MAC) addresses, and Internet Protocol (IP) addresses.

Adhering to requirement 3.5.2, ScheduleTrain implements robust authentication processes for users, processes, and devices as a prerequisite for granting access to our systems. This includes the use of passwords, key cards, and cryptographic devices. In response to 3.5.3, we mandate multifactor authentication for both privileged and non-privileged accounts, incorporating a combination of factors like something the user knows (password/PIN), something the user has (token or cryptographic device), and something the user is (biometric data).

To counteract replay attacks as per 3.5.4, our system employs replay-resistant authentication mechanisms, utilizing protocols that use nonces or challenges for one-time authentications. We prevent the reuse of identifiers for a defined period (3.5.5) and disable identifiers after a specified period of inactivity (3.5.6), thus reducing the risk associated with dormant accounts.

Our security protocols enforce minimum password complexity and require a change in characters for new passwords (3.5.7). We also prohibit password reuse for a specified number of generations (3.5.8) and enable temporary password use for system logons with an immediate mandate for change to a permanent password (3.5.9). Ensuring the security of password storage and transmission, ScheduleTrain only stores and transmits passwords that are cryptographically protected (3.5.10). Lastly, in line with 3.5.11, our system obscures feedback of authentication information to prevent unauthorized observation or compromise during the authentication process.

These comprehensive identification and authentication protocols underscore our commitment to maintaining the highest standards of security for CUI within ScheduleTrain.

3.6: Incident response

In adherence to Section 3.6 "Incident Response", ScheduleTrain has developed a comprehensive incident response capability that encompasses preparation, detection, analysis, containment, recovery, and user response activities as outlined in requirement 3.6.1. Our incident response plan is integrally designed with our systems and mission/business processes. We have established a robust mechanism for incident-related information gathering, which includes audit and network monitoring, physical access surveillance, and reports from users and administrators. Our incident handling capability is coordinated across various organizational entities, including system owners, legal departments, human resources, and risk management teams.

As part of our user response activities, we provide tailored incident response training to our personnel, aligned with their specific roles and responsibilities. This training ranges from basic incident recognition and reporting for regular users to more advanced incident handling and remediation techniques for system administrators and incident responders. Additionally, we offer support services such as help desk assistance and access to forensic services when required.

In line with requirement 3.6.2, we have procedures in place for tracking, documenting, and reporting incidents to both internal officials and external authorities as necessary. This process ensures that each incident is recorded in detail, providing valuable information for forensics, trend analysis, and incident management. Our reporting protocols are designed to comply with relevant laws, directives, and policies, ensuring timely and accurate communication of security incidents.

Furthermore, to ensure the effectiveness of our incident response capabilities, we conduct regular tests as stipulated in 3.6.3. These tests include a variety of exercises such as simulations, tabletop exercises, and comprehensive drills to identify any potential weaknesses or deficiencies in our response. The testing also helps us evaluate the potential impact of incident response on operations, assets, and personnel.

Through these measures, we ensure a robust and effective incident response mechanism that not only complies with the guidelines of SP 800-171, Revision 2 but also equips us to efficiently handle and mitigate any security incidents, thus safeguarding the CUI managed by ScheduleTrain.

3.7: Maintenance

In compliance with Section 3.7 "Maintenance", ScheduleTrain has implemented rigorous maintenance procedures to ensure the security and integrity of systems, which process CUI. Addressing requirement 3.7.1, we conduct regular and thorough maintenance of all system components, including hardware, firmware, and applications, regardless of whether they are directly associated with information processing or data retention. This encompasses devices such as scanners, copiers, and printers as well.

Maintenance can be divided into 2 areas: A: application maintenance, and B: Individual squadron maintenance. Application maintenance is handled by ScheduleTrain administrators exclusively. It’s the mechanism by which functionality is added, problems are fixed, and engineering specifications are changed. It takes the form of code pushed to the ScheduleTrain servers. Individual squadron maintenance is performed by squadron schedulers using the permissions granted them in the application by administrators. It includes managing individual permissions in their squadron, adding new users, transferring users to other squadrons, and deactivating accounts.

In line with 3.7.2, we maintain strict controls over the tools, techniques, mechanisms, and personnel used for system maintenance. We recognize that maintenance tools, whether they are hardware, software, or firmware, could potentially introduce malicious code. Therefore, we have established protocols for approving, controlling, and monitoring the use of these tools. Our approach includes regular checks for potential security risks associated with maintenance tools and actions.

To address the requirement of 3.7.3, we ensure that any equipment removed for off-site maintenance is completely sanitized of all CUI. This is to prevent any unauthorized access or disclosure of sensitive information during the maintenance process. Our sanitization processes align with the guidelines provided in [SP 800-88] on media sanitization.

In compliance with 3.7.4, we rigorously inspect media containing diagnostic and test programs for any malicious code before these media are used. In the event that malicious code is detected, we handle the incident in accordance with our established incident handling policies and procedures.

As stipulated in 3.7.5, we require multifactor authentication for establishing nonlocal maintenance sessions via external network connections and ensure these connections are terminated immediately after the maintenance activities are complete. This practice is in line with the network access requirements detailed in 3.5.3.

Finally, in accordance with 3.7.6, we supervise the maintenance activities of personnel who do not have the required access authorization. This applies to external individuals such as vendors or consultants who may need temporary privileged access to perform maintenance activities. We issue temporary credentials based on our risk assessments and ensure these credentials are strictly time-bound and monitored.

Through these comprehensive maintenance practices, we ensure the ongoing security and integrity of our systems, thereby safeguarding the CUI handled by ScheduleTrain.

3.8: Media protection

In compliance with Section 3.8 "Media Protection", ScheduleTrain enforces stringent media protection policies and practices to safeguard CUI on both digital and non-digital media.

Addressing requirement 3.8.1, we ensure the physical control and secure storage of all system media containing CUI. This includes digital media like hard drives, flash drives, CDs, and DVDs, as well as non-digital media such as paper. We limit access to these media to authorized personnel only and employ secure storage solutions such as locked cabinets or controlled media libraries.

In line with 3.8.2, access to CUI on system media is strictly limited to authorized users. We maintain strict control over these media through regular inventories, check-out and return procedures in our media library, and accountability for all stored media.

To fulfill 3.8.3, we sanitize or destroy system media containing CUI before disposal or release for reuse. This process ensures that CUI is irretrievable from the media, using sanitization techniques like clearing, purging, cryptographic erase, and physical destruction, in compliance with [SP 800-88] guidelines.

As per 3.8.4, we encourage that all media containing CUI are marked with the necessary security markings and distribution limitations, reflecting applicable laws and regulations.

Regarding 3.8.5, we control and maintain accountability for media containing CUI during transport outside of controlled areas. This includes the use of locked containers and cryptographic protections, as well as restricting transport activities to authorized personnel.

In accordance with 3.8.6, we implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport, unless alternative physical safeguards are in place. In particular, authentication in ScheduleTrain is handled using salted pbkdf2_sha256 algorithms, with 320,000 iterations.

In response to 3.8.7, we control the use of removable media on system components. This includes technical and non-technical controls to restrict or prohibit the use of devices like flash drives or external hard drives, and limiting the use of portable storage devices to approved devices only.

Per 3.8.8, we prohibit the use of portable storage devices that do not have an identifiable owner, thereby reducing the risk of malicious code insertion and other vulnerabilities.

Finally, as stipulated in 3.8.9, we ensure the confidentiality of backup CUI at storage locations. This is achieved through the use of cryptographic mechanisms or physical controls to protect the backup information.

Through these comprehensive media protection strategies, we ensure the secure handling, storage, and transport of all media containing CUI, thus safeguarding the integrity and confidentiality of this sensitive data within ScheduleTrain.

3.9: Personnel security

In line with Section 3.9 "Personnel Security", ScheduleTrain, primarily used by active-duty military officers including fighter pilots, has established comprehensive personnel security measures to ensure the protection of CUI.

Addressing requirement 3.9.1, we conduct thorough screening of individuals before granting them access to systems containing CUI. This screening process involves evaluating the conduct, integrity, judgment, loyalty, reliability, and stability of individuals, aligning with the trustworthiness criteria required for access to CUI. Our vetting process is in strict compliance with applicable federal laws, Executive Orders, directives, policies, and regulations. This approach is particularly crucial given the sensitive nature of our users' roles in military operations.

In compliance with 3.9.2, we ensure that our systems containing CUI are protected during and after personnel actions such as terminations and transfers. This includes the collection of system-related property from individuals who are leaving the organization or transferring to different roles. System-related property can include items such as hardware authentication tokens, identification cards, technical manuals, keys, and building passes.

Additionally, we ensure that access to official records and systems is appropriately modified to reflect the individual's new role or termination status. This comprehensive approach to personnel security is critical for maintaining the integrity and confidentiality of CUI, especially considering the high-security requirements associated with our user base of military personnel.

3.10: Physical protection

In accordance with Section 3.10 "Physical Protection", ScheduleTrain, used primarily by military squadrons and wings, adheres to stringent physical security measures to safeguard organizational systems, equipment, and CUI. This is consistent with the high level of care applied to handling other sensitive information such as flight records, address rosters, and training records.

Addressing requirement 3.10.1, we limit physical access to systems and equipment related to ScheduleTrain to authorized individuals only. This includes employees, individuals with permanent physical access authorization credentials, and visitors, all of whom are required to have proper authorization credentials like badges, identification cards, and smart cards. Physical access to equipment, such as computing devices, external disk drives, and networking devices, is restricted to locked rooms or secured areas accessible only to authorized personnel.

In compliance with 3.10.2, we ensure the protection and monitoring of the physical facility and support infrastructure for our systems. This includes employing security measures like guards, sensor devices, or video surveillance equipment. We also apply security controls to prevent accidental damage, disruption, physical tampering, eavesdropping, or modification of unencrypted transmissions to support infrastructure like wiring closets and cabling.

As per 3.10.3, visitors are escorted and their activities monitored within our facilities. This ensures that individuals without permanent physical access authorization are appropriately supervised, and their presence is logged for security purposes.

In line with 3.10.4, we maintain audit logs of physical access to our facilities. These logs can be procedural, automated, or a combination of both, documenting individual access to various physical access points within the facility.

Regarding 3.10.5, we exercise strict control and management of physical access devices such as keys, locks, combinations, and card readers. This ensures that access to sensitive areas and equipment is securely managed.

Finally, addressing 3.10.6, we enforce safeguarding measures for CUI at alternate work sites, which may include government facilities or private residences of employees. The security requirements for these alternate work sites are defined based on the work-related activities conducted at those sites, in accordance with guidance from [SP 800-46] and [SP 800-114] on enterprise and user security for teleworking.

Through these comprehensive physical security measures, we ensure the protection of systems and the CUI they handle, mirroring the stringent security practices of our military user base.

3.11: Risk assessment

In compliance with Section 3.11 "Risk Assessment" of SP 800-171, Revision 2, ScheduleTrain, utilized primarily by military squadrons and wings, incorporates a robust risk assessment framework to safeguard organizational operations and the CUI related to training plans and flight schedules.

Adhering to requirement 3.11.1, we periodically assess risks to US operations, assets, and individuals arising from the operation of our systems and the handling of CUI. This risk assessment process includes evaluating threats, vulnerabilities, likelihood, and impact, considering the potential risks from adversaries who might seek information about our training plans and flight schedules. We conduct these risk assessments at various levels—organization, mission/business process, and system—and throughout different phases of the system development life cycle, in line with guidance from [SP 800-30].

In line with 3.11.2, we routinely scan for vulnerabilities in our systems and applications, both periodically and when new vulnerabilities that could affect our systems are identified. This includes scanning for issues in all system components, such as networked printers and scanners, and ensuring the vulnerabilities are updated promptly as new threats are discovered. Our approach includes various analysis methods such as static, dynamic, and binary analysis for custom software applications. We employ tools and practices for vulnerability scanning that align with standards like the Security Content Automated Protocol (SCAP), the Common Vulnerabilities and Exposures (CVE) naming convention, and the Open Vulnerability Assessment Language (OVAL). We also reference sources such as the Common Weakness Enumeration (CWE) and the National Vulnerability Database (NVD) for vulnerability information. In certain sensitive cases, privileged access authorization facilitates thorough and secure vulnerability scanning, following the guidelines provided in [SP 800-40].

As per 3.11.3, vulnerabilities identified through our scanning processes are remediated in accordance with our risk assessments. This involves prioritizing remediation efforts and allocating the appropriate level of effort based on the assessed risk associated with each vulnerability.

Through this comprehensive risk assessment and vulnerability management approach, we ensure that risks to our systems and the sensitive CUI they handle, particularly regarding military training plans and flight schedules, are effectively identified, evaluated, and mitigated, thus maintaining the security and integrity of our operations.

3.12: Security assessment

In adherence to Section 3.12 "Security Assessment" of SP 800-171, Revision 2, ScheduleTrain, extensively utilized by military personnel, including fighter pilots, incorporates a thorough security assessment process. This process is critical, considering the potential risks such as adversaries gaining insight into training plans and flight schedules.

Addressing requirement 3.12.1, we periodically assess the security controls in operational systems to verify their effectiveness. This involves an evaluation of the safeguards or countermeasures implemented to satisfy security requirements. Our assessment process is integral to the system development life cycle, aiming to identify weaknesses and deficiencies early and provide essential information for risk-based decisions. These assessments are documented in detail, allowing for a clear understanding of whether the security controls are correctly implemented, operating as intended, and meeting security requirements. We follow the guidance provided in [SP 800-53] for security and privacy controls and [SP 800-53A] for conducting security assessments.

In line with 3.12.2, we develop and implement plans of action to correct deficiencies and reduce vulnerabilities in our systems. These plans describe how unimplemented security requirements will be met and how planned mitigations will be executed. We ensure that these plans are periodically updated and serve as critical inputs for risk management decisions regarding the processing, storing, or transmitting of CUI.

As per 3.12.3, we monitor our security controls continuously to ensure their ongoing effectiveness. This continuous monitoring program helps maintain awareness of threats, vulnerabilities, and information security, facilitating informed risk management decisions. We align this monitoring with the guidance provided in [SP 800-137], ensuring that the outputs are specific, measurable, actionable, relevant, and timely.

Finally, addressing 3.12.4, we develop, document, and periodically update system security plans. These plans describe system boundaries, environments of operation, the implementation of security requirements, and connections to other systems. The security plans, which can be a collection of various documents, contain sufficient information to enable a design and implementation that complies with the plans' intent and allows for risk determinations. Our approach to documenting these plans is guided by [SP 800-18].

Through this comprehensive security assessment approach, we ensure the ongoing effectiveness of our security controls, thereby safeguarding systems and the sensitive CUI they contain, particularly in the context of the high-security needs of our military user base.

3.13: System and communications protection

In compliance with Section 3.13 "System and Communications Protection", ScheduleTrain, widely used on computers managed by squadron scheduling shops, personal computers, and cell phones, adheres to stringent security measures to protect communications and system integrity.

Requirement 3.13.1 mandates monitoring, controlling, and protecting communications at key internal and external boundaries of organizational systems. We implement this through boundary components like gateways, routers, firewalls, and encrypted tunnels, ensuring secure communication channels. This is critical, considering the operational necessity of ScheduleTrain on various devices and the potential risks of adversaries targeting training and flight schedules.

In line with 3.13.2, we employ architectural designs, software development techniques, and systems engineering principles that bolster information security. This includes layered protections, embedding security policies and controls in design, and incorporating security requirements throughout the system development life cycle. Guidance from [SP 800-160-1] on systems security engineering informs our approach.

Addressing 3.13.3, we separate user functionality from system management functionality, ensuring that system administration tasks require privileged access, thus reducing the risk of unauthorized access or manipulation.

Requirement 3.13.4 focuses on preventing unauthorized information transfer via shared system resources. We control information in shared resources to prevent data leakage from prior users or roles to current users.

As per 3.13.5, we implement subnetworks or demilitarized zones (DMZs) for publicly accessible system components, physically or logically separated from internal networks, guided by [SP 800-41] and [SP 800-125B].

In accordance with 3.13.6, we enforce a policy of denying all network communications traffic by default and allowing traffic by exception, ensuring only essential connections are permitted.

Requirement 3.13.7 addresses the prevention of split tunneling in remote devices, crucial for devices like smartphones and tablets used in operational settings.

For 3.13.8, we implement cryptographic mechanisms to safeguard the confidentiality of CUI during transmission, in line with [NIST CRYPTO].

Addressing 3.13.9, we ensure that network connections are terminated at the end of sessions or after a defined period of inactivity to safeguard against unauthorized access.

Per 3.13.10, we manage cryptographic keys effectively, adhering to guidance from [SP 800-56A] and [SP 800-57-1].

In line with 3.13.11, we use FIPS-validated cryptography for protecting CUI, as prescribed in [NIST CRYPTO].

Requirement 3.13.12 focuses on preventing remote activation of collaborative computing devices, ensuring indications are provided to users when devices are in use.

3.14: System and information integrity

In accordance with Section 3.14 "System and Information Integrity", ScheduleTrain, primarily used on squadron scheduling computers, personal computers, and cell phones, adheres to stringent security measures to ensure system and information integrity.

Requirement 3.14.1 mandates the timely identification, reporting, and correction of system flaws. We actively identify systems affected by announced software flaws, including potential vulnerabilities, and report these to designated personnel with information security responsibilities. This includes updating security-relevant software and firmware in a timely manner, as guided by [SP 800-40] on patch management.

In line with 3.14.2, we provide protection from malicious code at designated locations within organizational systems. This includes implementing anti-virus and other malicious code protection mechanisms at critical points like firewalls, servers, and mobile devices, following guidance from [SP

800-83] on malware incident prevention.

As per 3.14.3, we monitor system security alerts and advisories and respond appropriately. This involves staying informed through sources like the Cybersecurity and Infrastructure Security Agency (CISA).

David O’Connor,
Founder of ScheduleTrain
Owner of Ops Plans, LLC