Tailoring NIST Security Controls for the Ground System: Selection and Implementation – Recommendations for Information System Owners

Eduardo Takamura[1] and Kevin Mangum[2]
NASA Goddard Space Flight Center, Greenbelt, MD 20770

The National Aeronautics and Space Administration (NASA) invests millions of dollars in spacecraft and ground system development, and in mission operations in the pursuit of scientific knowledge of the universe. In recent years, NASA sent a probe to Mars to study the Red Planet's upper atmosphere, obtained high resolution images of Pluto, and it is currently preparing to find new exoplanets, rendezvous with an asteroid, and bring a sample of the asteroid back to Earth for analysis. The success of these missions is enabled by *mission assurance*. In turn, mission assurance is backed by *information assurance*. The information systems supporting NASA missions must be reliable as well as secure. NASA – like every other U.S. Federal Government agency – is required to manage the security of its information systems according to federal mandates, the most prominent being the Federal Information Security Management Act (FISMA) of 2002 and the legislative updates that followed it. Like the management of enterprise information technology (IT), federal information security management takes a "one-size fits all" approach for protecting IT systems. While this approach works for most organizations, it does not effectively translate into security of highly specialized systems such as those supporting NASA missions. These systems include command and control (C&C) systems, spacecraft and instrument simulators, and other elements comprising the ground segment. They must be carefully configured, monitored and maintained, sometimes for several years past the missions' initially planned life expectancy, to ensure the ground system is protected and remains operational without any compromise of its confidentiality, integrity and availability. Enterprise policies, processes, procedures and products, if not effectively tailored to meet mission requirements, may not offer the needed security for protecting the information system, and they may even become disruptive to mission operations. Certain protective measures for the general enterprise may not be as efficient within the ground segment. This is what the authors have concluded through observations and analysis of patterns identified from the various security assessments performed on NASA missions such as MAVEN, OSIRIS-REx, New Horizons and TESS, to name a few. The security audits confirmed that the framework for managing information system security developed by the National Institute of Standards and Technology (NIST) for the federal government, and adopted by NASA, is indeed effective. However, the selection of the technical, operational and management security controls offered by the NIST model – and how they are implemented – does not always fit the nature and the environment where the ground system operates in even though there is no apparent impact on mission success. The authors observed that unfit controls, that is, controls that are not necessarily applicable or sufficiently effective in protecting the mission systems, are often selected to facilitate compliance with security requirements and organizational expectations even if the selected controls offer minimum or non-existent protection. This paper identifies some of the standard security controls that can in fact protect the ground system, and which of them offer little or no benefit at all. It offers multiple scenarios from real security audits in which the controls are not effective without, of course, disclosing any sensitive information about the missions assessed. In addition to selection and implementation of controls, the paper also discusses potential

[1] Information System Security Engineer (ISSE), General Dynamics Mission Systems (GDMS), non-member.
[2] Information System Security Officer (ISSO), General Dynamics Mission Systems (GDMS), non-member.

impact of recent legislation such as the Federal Information Security Modernization Act (FISMA) of 2014 – aimed at the enterprise – on the ground system, and offers other recommendations to Information System Owners (ISOs).

I. Introduction

THROUGH various security assessments of NASA information systems, specifically systems supporting ground systems and mission operations (GS/MO), and through the day-to-day security service in support of these systems, the authors have observed an ever present conflict between security compliance and (actual) security risk reduction. Some organizations[3] that participated in these security assessments have displayed sole interest in compliance with security requirements over the actual reduction of information technology (IT) risks. It is still a valid approach to security as being compliant will ensure the organization meets higher level requirements. These higher level requirements aim to assure the confidentiality, integrity and availability of the information system. Unfortunately, some of these requirements are intended for the overall security of enterprise IT, and may not be necessarily appropriate for specialized systems such as those supporting the ground system and mission operations. In fact, meeting certain security requirements aimed at the enterprise at large may even pose new risks to these specialized systems and therefore to the missions.

Security compliance is a must, and is what security auditors check for, but being compliant is not the same as being secure. Once security controls are in place, the identification, analysis, mitigation and tracking of risks – which are part of risk management activities – will actually provide the strongest protection to the information system provided they are performed on an on-going basis. According to a March 2016 federal cybersecurity survey[4] by $(ISC)^2$, "cybersecurity is quickly moving away from a 'one size fits all' set of standards, but the many compliance requirements do not allow for sufficient customization." For missions, this customization includes the tailoring of the security controls to better fit the unique environment in which they operate in. Unfortunately, some organizations overlook the tailoring of the security controls which occurs in one of the early phases of the security life cycle[5]. As a result, organizations try to make their information systems fit the controls and not the other way around as it should be. During security assessments[6], it becomes clear that the force-fitting of controls can have an impact on both compliance and risk reduction. It is important to understand each step of the RMF including the SELECTION step in which the baseline security controls are tailored. By tailoring the controls, the organization is ensuring that the most appropriate set of controls and control implementations are selected for the information system. This also facilitates the implementation of the controls as well as the assessment of the controls, ultimately leading to an authorization to operate (ATO).

While this paper will not go over the tailoring process, it will enumerate some of the security controls that could be tailored for the ground system and mission operations based on the generic, almost universal ground segment architecture design and configuration. The intent of the paper is to promote awareness of the tailoring process as well as to provide ISOs with an opportunity to reflect upon the selection of specific security controls that could be customized for the ground system and mission operations. The recommended customizations provided are meant to illustrate and emphasize the rationale behind the tailoring of the controls so that ISOs can apply similar concepts early in the RMF implementation or as part of the continuous monitoring process.

Scope

The recommendations herein emanated from lessons learned from security assessments of federal information systems, in particular of elements comprising NASA ground systems. The assessments were performed both prior to operations (i.e., prior to launch) and during operations. Non-mission information systems (e.g.,

[3] Missions, projects, partners in industry and academia.
[4] "The State of Cybersecurity from the Federal Cyber Executive Perspective," $(ISC)^2$ survey report [online], URL: https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/US_Government/ISC2-Federal-Cyber-Survey-Report.pdf [cited 07 August 2016].
[5] Step 2 of the NIST Risk Management Framework: SELECTION.
[6] Step 4 of the RMF: ASSESSMENT.

enterprise/corporate systems) were out of scope of the assessments. Nonetheless, organizations that have adopted or that are in the process of adopting the NIST Risk Management Framework (RMF) could benefit from the focus of this paper, specifically through the reviews of the rationale for each of the recommended tailoring proposed herein. ISOs from non-federal information systems could also benefit from this discussion if they have or will be adopting the RMF, the NIST Cybersecurity Framework, or other risk model. Regardless, ISOs must fully understand the mission, the environment in which the mission operates in, and the resources available to them so the tailoring process is completed successfully and effectively.

Assumptions

The focus of this paper is on the selection and implementation of (NIST Special Publication (SP) 800-53 revision 4 MODERATE[7]) security controls as part of the NIST RMF. The authors assume that other steps of the security life cycle are performed correctly. It is also assumed that the RMF model and its security controls[8] will change over time; however, the selection and implementation rationale may remain the same. The authors assume organizations have resources for the management and the support of information security, and have a working knowledge of the federal information security life cycle. Also, the elements that are mentioned throughout the paper are entities that comprise the ground system, and are operated by organizations. These organizations are NASA centers, NASA projects/missions, laboratories, universities, private companies, etc.

Disclaimer

While many organizations perform some customization/tailoring of security controls, some still oversee this important step of the security life cycle from the RMF. This paper intends to identify a few of the security controls that may be considered to be tailored to better protect and support the ground segment with focus on mission development and operations. Just like the idea of having a one size fits all for enterprise IT security brings challenges and concerns, the recommended tailoring proposed herein may not fit all like environments, and must be analyzed prior to implementation. In other words, these are only recommendations for customization; in fact, these recommendations are intended for ISOs of elements supporting the ground segment to consider when selecting the security controls for their information systems.

This is not a recipe for selecting and implementing security controls, but rather considerations for reference. Also, organizations should not be limited to the controls in the NIST SP 800-53 catalog[9]. Consider other security controls if applicable and as necessary. Finally, throughout this paper, some illustrations from actual security assessment findings will be provided to assist in the understanding of a given point. These cannot be traced back to any specific organization as such information is kept confidential for the protection of the assessed organization.

II. The Ground System

The ground system is comprised of multiple elements, each responsible for a specific aspect of the mission: Mission operations, science operations, ground stations, launch site, etc. Each element may be operated by a different organization (NASA centers, universities, laboratories, corporations). Needless to say, each element, and the mission network(s) connecting them are and must remain protected from unauthorized access and disruption. Most mission-agnostic elements such as ground stations, mission network service providers, launch service providers, etc. are already highly compliant with federal security requirements. Non-mission-agnostic elements such as Mission Operations Centers (MOCs), Science Operation Centers (SOCs), and Instrument Team Facilities (ITFs) may barely be compliant with federal security requirements, and these are the elements that the authors aim to reach with this publication.

[7] Most missions information systems are categorized as MODERATE.
[8] As of the time of this writing, the controls were from the NIST SP 800-53 revision 4 security control catalog.
[9] NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations [online], URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [cited 12 August 2016].

III. The Security Life Cycle

The Risk Management Framework (RMF) is a 6-step cycle aimed at selecting, applying, and verifying the appropriate security controls to provide confidentiality, integrity and availability assurance to federal information systems, and continuously monitoring the effectiveness of these controls. The level of protection required to provide confidentiality, integrity and availability assurance to the information system will depend on the value of the data/information to be protected. Therefore, the security life cycle begins with the categorization of the data based on the type of information. The output of the categorization process, described in SP 800-60 and Federal Information Processing Standard (FIPS) 199, is either LOW, MODERATE or HIGH security rating. For each rating, NIST provides security control baselines that can be tailored during the selection step of the security life cycle. Most of the baselined security controls from catalog are acceptable by organizations to meet minimum security requirements. After the controls are implemented, they must be assessed to verify compliance and effectiveness. After the implementation evaluation results and residual risks are reviewed and accepted, the information is ultimately authorized to operate. Once the information system is authorized, it must be continuously monitored to ensure controls are still applicable, relevant and effective. A description of each RMF step can be found in chapter 3 of NIST SP 800-37[10].

Table I The 6-step NIST Risk Management Framework (RMF)

NIST Risk Management Framework
Step 1: CATEGORIZE Information Systems (FIPS 199/SP 800-60)
Step 2: SELECT Security Controls (FIPS 200/SP 800-53)
Step 3: IMPLEMENT Security Controls (SP 800-160)
Step 4: ASSESS Security Controls (SP 800-53A)
Step 5: AUTHORIZE Information Systems (SP 800-37)
Step 6: MONITOR Security Controls (SP 800-137)

IV. The Tailoring Process

Organizations implementing the NIST RMF can certainly benefit from the security in-depth (layered) approach that the model offers, in particular by the technical, operational and management controls from the NIST baseline security control catalog. Because of the interdependencies between the controls, it is advisable to not only select as many controls as applicable to the security rating[11] of the system but also fully implement them if at all possible. When it is not possible to fully implement the controls as recommended by NIST even when the controls are applicable to the system, then is its necessary to customize the controls.

Tailoring of the controls is necessary to avoid force-fitting them to support the unique environment and operations of the ground system. This important step of the SELECTION phase can assist in the understanding and implementation of the controls as well as facilitate the assessment of the controls.

[10] NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach [online], URL: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf [cited 12 August 2016].

[11] Security Categorization

The tailoring process is summarized as follows:

Table 2 The Tailoring Process

- Identify and designate common controls in initial security control baselines;
- Apply scoping considerations to the remaining baseline security controls;
- Select compensating security controls (if needed)
- Assign specific values to organization-defined security control parameters via explicit assignment and selection statements;
- Supplement baselines with additional security controls and control enhancements (if needed); and
- Provide additional specification information for control implementation (if needed).

For a description and explanation of the tailoring process, see section 3.2 of NIST SP 800-53 Revision 4[12].

Tailored controls need to be documented in the system security plan (SSP), and verification systems (e.g., vulnerability scanners) configured accordingly. The idea is to document deviations in support of not only the implementation of the controls but in the verification of the controls during the security assessment and continuous monitoring steps.

V. Tailoring Select Security Controls by Key Security Groups

Once security controls are selected from the NIST SP 800-53 catalog (step 2 of the Risk Management Framework security lifecycle), the organization must determine its Organization-Defined Values (ODVs). Without these values, projects have little or no implementation guidance. Also, without these, audits can become very challenging as one cannot verify a requirement is being met if the requirement is only partially defined.

Organizations must ensure that policies are in place for all security control families. These are the first controls of each security control family in the catalog ("XX-1 controls" where XX is the abbreviation of the security control family). Like ODVs, policies must be well defined, accessible, understood, and auditable or else they cannot be followed and/or enforced. Unfortunately, some policies are not tailored enough for the ground system and mission operations environment. At times, they are not tailored at all for such environment making it difficult to implement and assess[13].

[12] NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations [online], URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [cited 12 August 2016].
[13] Subsequent steps 3 and 4 of the NIST Risk Management Framework (RMF).

The following is a collection of candidate controls to be tailored for the highly specialized systems supporting ground system and mission operations. Each control family has been grouped under the following security groups:

A. ACCESS CONTROL
B. CONFIGURATION MANAGEMENT
C. MAINTENANCE AND MONITORING
D. MANAGEMENT AND SUPPORT

These groups (not to be confused with the security control families of the same/similar names) are aligned with the key security groups proposed by Takamura et. al.[14] when implementing and assessing critical elements such as Mission Operations Centers (MOCs).

This compilation is a result of observed patterns from various security assessments performed on NASA ground systems and mission operations, and they do not reflect the current implementation of a single or multiple information systems. The intent is not to show how controls are being implemented but rather how it could be implemented taking into consideration the environment, the nature of operations, the processes that must be followed, etc.

Each control is listed as a table organized as following:

SECURITY CONTROL FAMILY	
Security Control Title *(XX-NN)* *(Where XX is the security control family abbreviation, and NN is the security control number)*	*NIST:* *Excerpt or entire control description.* *NIST supplemental guidance:* *Excerpt or entire supplemental guidance for the control.*
	Reality: *Description of the environment, the nature of operations, the processes that must be followed, etc. to substantiate the deviation and re-standardization of the control implementation.*
	Tailoring recommendation/rationale: *Suggested deviation and re-standardization of the control based on the above considerations.*

A. Access Control

ACCESS CONTROL	
Separation of Duties (AC-05)	NIST: The organization: (a) Separates [organization-defined duties of individuals]; (b) documents separation of duties of individuals; and (c) defines information system access authorizations to support separation of duties. NIST supplemental guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: [..] (iii) ensuring security personnel administering access control functions do not also administer audit functions.

[14] Takamura, E., Mangum, K., Wasiak, F., Gomez-Rosa, C., "Information Security Considerations for Protecting NASA Mission Operations Centers (MOCs)," 2015 IEEE Aerospace Conference, URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7119207 [cited 14 August 2016].

	Reality: In order to reduce costs, missions/projects assign some of the IT security roles and responsibilities to IT support personnel, which makes it difficult to observe the principle of separation of duties. The review of audit logs by System Administrators (SAs), for instance, could be viewed as a risk since SAs have elevated privileges on the system, thus the capability to delete audit records. Adding the role of audit log reviewers to SAs may be inevitable due to limited mission/project budget during operations and especially during extended mission life.
	Tailoring recommendation/rationale: If separation of duties is not possible, assign mission support personnel to perform random inspections/verifications to ensure privileges are not being misused or abused.
Unsuccessful Login Attempts (AC-07)	NIST: The information system: (a) Enforces a limit of [organization-defined number] consecutive invalid logon attempts by a user during a [organization-defined time period]; and (b) automatically [locks the account/node for an [organization-defined time period] | locks the account/node until released by an administrator | delays next logon prompt according to [organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded. NIST supplemental guidance: [..] Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations.
	Reality: Many of the ground system elements operate in a multi-user environment. Terminals cannot afford to be locked by a given operator (or even the unlikely unauthorized user) after a number of unsuccessful login attempts occur.
	Tailoring recommendation/rationale: To prevent accidental (or intentional) denial of service by any of the multiple operators (or by hackers), especially after a password is changed, but to meet the intent of the control, set the maximum number of unsuccessful attempts is set to a high number. For instance, instead of 10 failed attempts, set it to 50 or 100. This is only "safe to do so" if compensating controls are in place (e.g., segregated logical and physical environments each with controlled access).
System Use Notification (AC-08)	NIST: The information system: (a) Displays to users [organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance [..]. NIST supplemental guidance: System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist.
	Reality: Certain organizations have mandated that security warning labels be physically affixed to network printers. While it is possible to configure network printers to authenticate users, most of the printers supporting the GS/MO are not set-up to do so. For printers with a web user interface (WebUI), it may not be possible to edit the UI to display a security warning banner on the authentication/login page. Network printers within the LAN are protected by access controls.

	Tailoring recommendation/rationale: The intent of the control is to notify remote and local users – attempting to be authenticated – of the conditions and restrictions for accessing the device. Since access to network printers within the LAN does not require authentication, and because of the inability for proprietary web pages in the WebUI to be edited, the installation of banners on these devices can/should be waived. Compensating controls include segregated logical and physical environments each with controlled access.
Session Lock (AC-11)	NIST: The information system: (a) Prevents further access to the system by initiating a session lock after [organization-defined time period] of inactivity or upon receiving a request from a user; and (b) retains the session lock until the user reestablishes access using established identification and authentication procedures. NIST supplemental guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of the workdays.
	Reality: Some devices display information that require continuous viewing, and cannot/should not have sessions locked since it would defeat the purpose of the device.
	Tailoring recommendation/rationale: Identify the devices that cannot/should not have sessions locked; disable session locks on these devices; and remove/waive requirement from them. Compensating controls include segregated logical and physical environments each with controlled access.
Session Lock | Pattern-Hiding Displays (AC-11(1)	NIST: The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. NIST supplemental guidance: Publicly viewable images can include static or dynamics images, for example, patters used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.
	Reality: Some devices display information that require continuous viewing, and cannot/should not have sessions locked since it would defeat the purpose of the device.
	Tailoring recommendation/rationale: Identify the devices that cannot/should not have sessions locked; disable session locks on these devices; and remove/waive requirement from them. Compensating controls include segregated logical and physical environments each with controlled access.

Session Termination (AC-12)	NIST: The information system automatically terminates a user session after [organization-defined conditions or trigger events requiring session disconnect]. NIST supplemental guidance: This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect).
	Reality: Some devices display information that require continuous viewing, and cannot/should not have sessions terminated since it would defeat the purpose of the device.
	Tailoring recommendation/rationale: Identify the devices that cannot/should not have sessions terminated; disable automatic session termination on these devices; and remove/waive requirement from them. Compensating controls include segregated logical and physical environments each with controlled access.
Wireless Access (AC-18)	NIST: The organization: (a) Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and (b) authorizes wireless access to the information system prior to allowing such connections. NIST supplemental guidance: Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., (EAP/TLS, PEAP), which provide credential protection and mutual authentication.
	Reality: No Wi-Fi in support of operations.
	Tailoring recommendation/rationale: De-select control if Wi-Fi is not supported or permitted.
Publicly Accessible Content (AC-22)	NIST: The organization: (a) Designates individuals authorized to post information onto a publicly accessible information system; (b) trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; (c) reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and (d) reviews the content on the publicly accessible information system for nonpublic information [organization-defined frequency] and removes such information, if discovered. NIST supplemental guidance: In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by organizational policy.
	Reality: With the exception of data archiving elements, GS/MO elements do not offer publicly accessible content.
	Tailoring recommendation/rationale: De-select control if no publicly accessible content is offered.

IDENTIFICATION AND AUTHENTICATION (IA)	
Identification and Authentication | Acceptance of PIV Credentials IA-02(12)	NIST: The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials. NIST supplemental guidance: This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.
	Reality: The ground system is often comprised of elements operated by government, industry and academia. There is no federated solution for deploying personal identification verification (PIV) cards across the ground system to identify and authenticate users from all elements. Also, many of the ground system elements operate in a multi-user environment in which a single (group) account is needed so sessions span multiple shifts.
	Tailoring recommendation/rationale: De-select the control if PIV credentials cannot be utilized.
Identification and Authentication | Acceptance of PIV Credentials From Other Agencies (IA-8(1))	NIST: The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies. NIST supplemental guidance: This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.
	Reality: The ground system is often comprised of elements operated by government, industry and academia. There is no federated solution for deploying personal identification verification (PIV) cards across the ground system to identify and authenticate users from all elements and from other agencies. Also, many of the ground system elements operate in a multi-user environment in which a single (group) account is needed so sessions span multiple shifts.
	Tailoring recommendation/rationale: De-select the control if PIV credentials from other agencies cannot be utilized.

PHYSICAL AND ENVIRONMENTAL PROTECTION	
Physical Access Control (PE-03)	NIST: The organization: (a) Enforces physical access authorizations at [organization-defined entry/exist points to the facility where the information system resides] by: (1) verifying individual access authorizations before granting access to the facility; and (2) controlling ingress/egress to the facility using: [[organization-defined physical access control systems/devices] | guards]; (b) maintains physical access audit logs for [organization-defined entry/exit points]; (c) provides [organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible; (d) escorts visitors and monitors visitor activity [organization-defined circumstances requiring visitor escorts and monitoring]; (e) secures keys, combinations, and other physical access devices; (f) inventories [organization-defined physical access devices] every [organization-defined frequency]; and (g) changes combinations and keys [organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. NIST supplemental guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. [..] Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. [..]
	Reality: Many of the ground system elements (both NASA internal and NASA external information systems) operate in a multi-user environment where the same facilities are physically shared with multiple missions/projects. These elements are often located inside secure facilities, some of them are certified by the Department of Defense.
	Tailoring recommendation/rationale: If same physical facilities are shared with multiple projects/missions, perform risk assessment, but ensure intent of the control is observed/followed. Special attention should be given to individual mission/project access requirements, and whether the shared resources (facilities) could incur any unacceptable risks to individual missions/projects. Compensating controls may focus on personnel security, monitoring, and other pertinent physical security measures. Comments: Generally, missions/projects fare very well in the physical security aspect, especially if the organization is engaged in defense work such as the case of many of the laboratories with federal government contracts. Laboratories often demonstrate stronger physical security than universities.

B. Configuration Management

CONFIGURATION MANAGEMENT	
Baseline Configuration (CM-02(2))	NIST: The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. NIST supplemental guidance: Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. [..]
	Reality: Many elements are still manually configuring systems (this control enhancement is not selected for MODERATE systems).
	Tailoring recommendation/rationale: Although this control enhancement is not selected for MODERATE systems, elements should consider using automation for maintaining baseline configurations. Many organizations have successfully implemented virtualized environments that provide effective and easy to use tools for automating certain CM processes such as baseline configuration maintenance.
Baseline Configuration | Configure Systems, Components, or Devices for High-Risk Areas (CM-02(7))	NIST: The organization: (a) Issues [organization-defined information systems, system components, or devices] with [organization-defined configuration] to individuals traveling to locations that the organization deems to be of significant risk; and (b) applies [organization-defined security safeguards] to the devices when the individuals return. NIST supplemental guidance: When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. [..]
	Reality: Mobile devices are rarely utilized for operations. When they do, it is mostly for internal work, and they do not leave the premises.
	Tailoring recommendation/rationale: De-select control if devices do not leave the premises.

Configuration Change Control (CM-03)	NIST: The organization: (a) Determines the types of changes to the information system that are configuration-controlled; (b) reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; (c) documents configuration change decisions associated with the information system; (d) implements approved configuration-controlled changes to the information system; (e) retains records of configuration controlled-changes to the information system for [organization-defined time period]; (f) audits and reviews activities associated with configuration-controlled changes to the information system; and (g) coordinates and provides oversight for configuration change control activities through [organization-defined configuration change control element (e.g., committee, board] that convenes: [[organization-defined frequency] | [organization-defined configuration change conditions]]. NIST supplemental guidance: Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operation systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. [..]
	Reality: Some organizations overkill project-level Change Control Boards (CCBs) with low-level routine IT work that could be handled by a dedicated and specialized IT CCB.
	Tailoring recommendation/rationale: Establish a dedicated and specialized IT CCB to handle low-level routine IT work, but continue to engage project-level CCB for all other changes.
Security Impact Analysis (CM-04)	NIST: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. NIST supplemental guidance: Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. [..]
	Reality: Not enough SIA is performed.
	Tailoring recommendation/rationale: Incorporate SIA into change request and maintenance processes.

Configuration Settings (CM-06)	NIST: The organization: (a) Establishes and documents configuration settings for information technology products employed within the information system using [organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; (b) implements the configuration settings; (c) identifies, documents, and approves any deviations from established configuration settings for [organization-defined information system components] based on [organization-defined operational requirements]; and (d) monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. NIST supplemental guidance: Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. [..] Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. [..] Common secure configurations include the United States Government Configuration Baseline (USGCB) [..] The Security Content Automation Protocol (SCAP) and the defined standards within the protocol.
	Reality: Some organizations are still manually configuring devices, making it a time-consuming and laborious effort.
	Tailoring recommendation/rationale: Configure settings using automated protocols, preferably those that have been pre-configured by the organization (and with deviations and justifications already documented).
Information System Component Inventory (CM-08)	NIST: The organization: (a) Develops and documents an inventory of information system components that: (1) accurately reflects the current information system; (2) includes all components within the authorization boundary of the information system; (3) is at the level of granularity deemed necessary for tracking and reporting; and (4) includes [organization-defined information deemed necessary to achieve effective information system component accountability]; and (b) reviews and updates the information system component inventory [organization-defined frequency]. NIST supplemental guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems.
	Reality: Some organizations are still manually inventorying assets, making it a time-consuming and laborious effort.
	Tailoring recommendation/rationale: Credentialed vulnerability scan reports, if configured appropriately, may provide an automated method for obtaining information system component inventories.

MEDIA PROTECTION	
Media Marking (MP-03)	NIST: The organization: (a) Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and (b) exempts [organization-defined types of information system media] from marking as long as the media remain within [organization-defined controlled areas]. NIST supplemental guidance: The term security marking refers to the application/use of human-readable security attributes. [..]
	Reality: Some organizations utilize automated media handling hardware (e.g., tape drives, robotic media handlers, etc.) which may be sensitive to labels (e.g., SBU labels) affixed to the media that could potentially damage the hardware.
	Tailoring recommendation/rationale: Apply labels to protective case/enclosure or, if not possible (e.g., large volume of library), affix poster with markings to entry/exit point (i.e., storage door). Compensating control may include conditions and restrictions under which the media leaves (or not) the facility.

SYSTEM AND COMMUNICATIONS PROTECTION	
Network Disconnect (SC-10)	NIST: The information system terminates the network connection associated with a communications session at the end of the session or after [organization-defined time period] of inactivity. NIST supplemental guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.
	Reality: Most terminals cannot/should not be disconnected from the network at the end of a sessions or after a pre-determined period of inactivity.
	Tailoring recommendation/rationale: Identify the devices that cannot/should not be disconnected from the network (which is basically all of the assets); and remove/waive requirement from them. Compensating controls include segregated logical and physical environments each with controlled access.
Cryptographic Protection (SC-13)	NIST: The information system implements [organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. NIST supplemental guidance: Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. [..]

	Reality: Some elements utilize insecure protocols (e.g., FTP) when uploading non-sensitive data to an archive. The argument provided is that the data is not sensitive, and therefore does not need to be encrypted.
	Tailoring recommendation/rationale: Regardless of whether the data being transferred is sensitive or not, the user performing the uploading of the data needs to be authenticated, and the credentials utilized must be protected. Else, they can be sniffed, and acquired by anyone listening to the network(s) between the client and the server.
Collaborative Computing Devices (SC-15)	NIST: The information system: (a) Prohibits remote activation of collaborative computing devices with the following exceptions: [organization-defined exceptions where remote activation is to be allowed]; and (b) provides an explicit indication of use to users physically present at the devices. NIST supplemental guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. [..]
	Reality: Not used in GS/MO environments.
	Tailoring recommendation/rationale: De-select control (not applicable to the GS/MO environment). Comment: Mission/project personnel can collaborate using non-mission devices.
Session Authenticity (SC-23)	NIST: The information system protects the authenticity of communications sessions. NIST supplemental guidance: This control addresses communications protections at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.
	Reality: Some of the web applications in use within the GS/MO environment utilize self-signed Secure Sockets Layer (SSL) certificates.
	Tailoring recommendation/rationale: Self-signed SSL certificates OK as clients are generally in the same LAN as the web servers, and so the web server identities do not need to be verified by a Certification Authority (CA).
Protection of Information at Rest (SC-28)	NIST: The information system protects the [confidentiality | integrity] of [organization-defined information at rest]. NIST supplemental guidance: This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. [..]
	Reality: Most GS/MO devices are multi-user devices in multi-user environments; no mobile computing in general.

	Tailoring recommendation/rationale: Control only applicable to removable devices (e.g., USB thumbdrives) that require FIPS 140-2 validation.

PRIVACY	
Privacy Impact and Risk Assessment (AR-02)	NIST: The organization: (a) Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and (b) conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures. NIST supplemental guidance: Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. [..]
	Reality: In most cases, the ground system does not handle any private (personal) information.
	Tailoring recommendation/rationale: This is often an organizational control; elements may still be required to document whether private information is handled or not. If organization maintains a multi-mission SSP, this and other privacy controls should be tailored for all missions/projects.

C. Maintenance and Monitoring

AUDIT AND ACCOUNTABILITY	
Auditable Events (AU-02)	NIST: The organization: (a) Determines that the information system is capable of auditing the following events: [organization-defined auditable events]; (b) coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; (c) provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and (d) determines that the following events are to be audited within the information system: [organization-defined audited events (the subset of the auditable events defined in AU-02a) along with the frequency of (or situation requiring) auditing for each identified event]. NIST supplemental guidance: An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. [..]
	Reality: Many of the GS/MO devices run Linux/UNIX operating systems.

	Tailoring recommendation/rationale: If running default syslog service on Linux/UNIX and MacOS, the majority of the required auditable events are already enabled. Not applicable to Windows and application logging.
Response to Audit Processing Failures (AU-05)	NIST: The information system: (a) Alerts [organization-defined personnel or roles] in the event of an audit processing failure; and (b) takes the following additional actions: [organizational-defined actions to be taken (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records)]. NIST supplemental guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. [..]
	Reality: By design, mail service is disabled within GS/MO elements, but it is required to process mail in order to send notifications. Unless the service is enabled, and packets allowed through, individuals cannot be alerted.
	Tailoring recommendation/rationale: If mail service can be enabled, then automated notifications can be sent to security or support personnel; else, if it cannot be enabled, a compensating control could include daily review of audit logs.

SECURITY ASSESSMENT AND AUTHORIZATION	
Security Assessments (CA-02)	NIST: The organization: (a) Develops a security assessment plan that describes the scope of the assessment including: (1) security controls and control enhancements under assessment; (2) assessment procedures to be used to determine security control effectiveness; and (3) assessment environment, assessment team, and assessment roles and responsibilities; (b) assesses the security controls in the information system and its environment of operation [organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; (c) produces a security assessment report that documents the results of the assessment; and (d) provides the results of the security control assessment to [organization-defined individuals or roles]. NIST supplemental guidance: Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; (iv) system development life cycle activities. [..]
	Reality: Not all elements consider internal security assessments during their development.
	Tailoring recommendation/rationale: Initiate internal security assessments during the development of the GS/MO elements.

Penetration Testing (CA-08)	NIST: The organization conducts penetration testing [organization-defined frequency] on [organization-defined information systems or system components]. NIST supplemental guidance: Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. [..]
	Reality: Most missions/projects supporting GS/MO are categorized as MODERATE systems. Penetration testing is not required for MODERATE systems.
	Tailoring recommendation/rationale: Elements should consider conducting penetration testing during development and prior to operations. After operations, no penetration testing; instead, focus on monitoring and awareness training. Comment: The deviation, in this case, is to implement a security control that is required for HIGH rated systems.

MAINTENANCE	
System Maintenance Policy and Procedures (MA-01)	NIST: The organization: (a) Develops, documents, and disseminates to [organization-defined personnel or roles]: (1) a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and (b) reviews and updates the current: (1) system maintenance policy [organization-defined frequency]; and (2) system maintenance procedures [organization-defined frequency]. NIST supplemental guidance: This controls addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. [..]
	Reality: Successful missions often live long past their expected life, and their budgets remain limited or even decrease over the years. In order for the science aspect of the mission be prolonged, mission/project support and support personnel are phased out including system support. Also, certain processes such as documentation development are not followed since the personnel supporting the element are often "veteran" professionals having worked on previous missions.

	Tailoring recommendation/rationale: Mission management must be prepared to ensure the information technology supporting the mission keeps up with advances in technology. By keeping hardware and software updated, risks related to obsolesce are avoided. Potential problems include lack of funding for maintenance, technology refreshes, and support personnel for maintaining the information systems. About the lack of documentation (e.g., procedural documents) by seasoned support personnel, if there is low turnover of management and support staff, then the risk of not documenting certain procedures need to be reviewed, analyzed, documented and accepted. Tailoring, in this case, may not be helpful.

RISK ASSESSMENT	
Vulnerability Scanning (RA-05)	NIST: The organization: (a) Scans for vulnerabilities in the information system and hosted applications [organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; (b) employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: (1) enumerating platforms, software flaws, and improper configurations; (2) formatting checklists and test procedures; and (3) measuring vulnerability impact; (c) analyzes vulnerability scan reports and results from security control assessments; (d) remediates legitimate vulnerabilities [organization-defined response times] in accordance with an organizational assessment of risk; and (e) shares information obtained from the vulnerability scanning process and security control assessments with [organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). NIST supplemental guidance: Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. [..]
	Reality: Due to the nature of mission operations, GS/MO devices may not be capable of being scanned at the same pace as their general computing counterparts. Likewise, they are not patched as often since a more comprehensive risk analysis as well as testing are needed prior to the deployment of patches and updates. Some elements perform non-credentialed scanning only.
	Tailoring recommendation/rationale: Align vulnerability management with patch management processes. Credentialed vulnerability scanning is a must. Although technically feasible, centralized vulnerability scanning of all ground system elements is usually not performed (the scans are done locally). Multi-Mission Operations Centers (MMOC) should consider sharing resources such as vulnerability scanners, especially if the same personnel supports other missions. Comments: Each mission has its own schedule. Scanning should not be performed during, for instance, a spacecraft pass.

SYSTEM AND INFORMATION INTEGRITY	
Flaw Remediation (SI-02)	NIST: The organization: (a) Identifies, reports, and corrects information system flaws; (b) tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; (c) installs security-relevant software and firmware updates within [organization-defined time period] of the release of the updates; and (d) incorporates flaw remediation into the organizational configuration management process. NIST supplemental guidance: Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. [..]
	Reality: Due to the nature of mission operations, GS/MO devices may not be capable of being patched at the same pace as their general computing counterparts. A more comprehensive risk analysis as well as testing are needed prior to the deployment of patches and updates. Some mission assets cannot be patched/updated since they were built to simulate the software that is currently running on the spacecraft.
	Tailoring recommendation/rationale: Tailor the control to perform patching/updates at an interval that will not impact the mission. Compensating control may include strong configuration management processes. If patches cannot be deployed at least monthly, then every other month or every quarter. Because of the volume of patches/updates that accumulate each month, waiting longer than a quarter to deploy the patch is not advisable. The patch frequency tailored for GS/MO devices should also be coordinated with vulnerability assessment cadence so that the devices are scanned right after they are patched for more accurate results. Also, it is important to perform more extensively any testing before (and after) patching operational systems. For assets that cannot be updated, missions must identify and document compensating controls that offer protection to these vulnerable systems.

Malicious Code Protection (SI-03)	NIST: The organization: (a) Employs malicious code protection mechanisms at information system entry and exist points to detect and eradicate malicious code; (b) updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; (c) configures malicious code protection mechanisms to: (1) Perform periodic scans of the information system [organization-defined frequency] and real-time scans of files from external sources at [endpoint | network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and (2) [block malicious code | quarantine malicious code | send alert to administrator | [organization-defined action]] in response to malicious code detection; and (d) addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. NIST supplemental guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. [..]
	Reality: Many of the GS/MO devices runs Linux/UNIX operating systems. There is a perception that there is little value of running anti-virus software on these systems.
	Tailoring recommendation/rationale: There are viruses and worms for all computing platforms including mobile devices. On Linux/UNIX systems, most of the malware are only effective if the systems are running vulnerable software. If the elements keep the systems up-to-date with the latest patches/updates, the likelihood of these systems from becoming infected is very low. The fact that these systems are segregated logically and physically with controlled access drops the probability of infection to even lower levels. Even if auto-protection (aka., on-access virus scanning) is not available on these systems, elements may consider tailoring the control to waive the frequent full scanning, especially if files do not change often. As a result, unnecessary processes (e.g., weekly full virus scans) wearing out media storage (disks) will be avoided.
Spam Protection (SI-08)	NIST: The organization: (a) Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and (b) updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. NIST supplemental guidance: Information system entry and exist points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. [..]
	Reality: By design, mail service is disabled within GS/MO elements. If the service is enabled then access to the server is restricted.
	Tailoring recommendation/rationale: De-select this control is mail service is not enabled. If it is, ensure that the service only listens to the localhost (assuming service is enabled for internal use only).

D. Management and Support

AWARENESS AND TRAINING	
Role-Based Security Training (AT-03)	NIST: The organization provides role-based security training to personnel with assigned security roles and responsibilities; (a) before authorizing access to the information system or performing assigned duties; (b) when required by information system changes; and (c) [organization-defined frequency] thereafter. NIST supplemental guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. [..]
	Reality: Mission/project personnel assuming specific roles are not always trained (sometimes there are no training requirements for certain roles).
	Tailoring recommendation/rationale: System Administrators, Account Administrators, Developers, Database Administrators, Network Administrators, Security Administrators (ISSEs), Security Managers (ISSOs), Information System Owners (ISOs) should all take role-based security training at least once every 3 years. Comments: For missions on extended life, there is often a reduction in staff including IT support. As a result, support staff may take on IT and/or IT security roles which the staff may or may not be qualified (risk).
Role-Based Security Training (AT-03)	NIST: The organization provides role-based security training to personnel with assigned security roles and responsibilities; (a) before authorizing access to the information system or performing assigned duties; (b) when required by information system changes; and (c) [organization-defined frequency] thereafter. NIST supplemental guidance: Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. [..]
	Reality: Some organizations require personnel with specific roles (e.g., System Administrators) to take annual refresher training using static and often old materials.
	Tailoring recommendation/rationale: Because many of the specialized personnel are qualified personnel who are proficient in their craft, the annual requirement could be modified so that the refresher is only required every 3 years.

CONTINGENCY PLANNING	
Alternate Processing Site (CP-07)	NIST: The organization: (a) Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [organization-defined information system operations] for essential missions/business functions within [organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; (b) ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and (c) ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site. NIST supplemental guidance: Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available.
	Reality: Depending on the class of the mission, elements may or may not have an alternate processing site, that is, a backup site. In many cases, there are no alternate processing sites.
	Tailoring recommendation/rationale: If an alternate processing site does not exist, then the element must ensure its configuration management and contingency planning processes addresses many of the concerns related to element availability. The important of an alternate storage site increases when a backup site does not exist or is not available.
Information System Backup (CP-09)	NIST: The organization: (a) Conducts backups of user-level information contained in the information system [organization-defined frequency consistent with recovery time and recovery point objectives]; (b) conducts backups of system-level information contained in the information system [organization-defined frequency consistent with recovery time and recovery point objectives]; (c) conducts backups of information system documentation including security-related documentation [organization-defined frequency consistent with recovery time and recovery point objectives]; and (d) protects the confidentiality, integrity, and availability of backup information at storage locations. NIST supplemental guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. [..]
	Reality: Many organizations place emphasis on having hot sites for their key elements (e.g., mission operations centers); however, when hot sites do not exist, CP is often "dismissed." The only remaining protective measure seems to be data backups.
	Tailoring recommendation/rationale: Backups are important, and must be performed whether an alternate processing site exists or not. They should be part of the CM process in case data is to be restored after a failed change to the system.

INCIDENT RESPONSE	
Incident Reporting (IR-06)	NIST: The organization: (a) Requires personnel to report suspected security incidents to the organizational incident response capability within [organization-defined time period]; and (b) reports security incident information to [organization-defined authorities]. NIST supplemental guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. [..]
	Reality: Each element has its own incident reporting process, and not unified response line (for the ground system).
	Tailoring recommendation/rationale: Ensure the Ground System ISSO is added to the IR process.

PLANNING	
System Security Plan (PL-02)	NIST: The organization: (a) Develops a security plan for the information system [..]; (b) distributes copies of the security plan and communicates subsequent changes to the plan to [organization-defined personnel or roles]; (c) reviews the security plan for the information system [organization-defined frequency]; (d) updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and (e) protects the security plan from unauthorized disclosure and modification. NIST supplemental guidance: Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. [..]
	Reality: Some organizations support multiple missions/projects, but each has its own SSP and defined values (parameters), sometimes differing from each other's implementation.
	Tailoring recommendation/rationale: Elements whose operators support multiple missions/projects should consider creating a single system security plan (SSP) for all missions/projects, especially if the missions/projects share the same resources (physical location, support personnel, infrastructure, IT assets, etc.). This also helps reduce assessment and authorization (A&A) costs.

PERSONNEL SECURITY	
Personnel Screening (PS-03)	NIST: The organization: (a) Screens individuals prior to authorizing access to the information system; and (b) rescreens individuals according to [organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening]. NIST supplemental guidance: Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.
	Reality: Some (non-NASA) organizations offer resistance in screening their personnel.
	Tailoring recommendation/rationale: Personnel screening is an important aspect of personnel security. While background checks may or may not be indicative of personnel security and trustworthiness, all personnel requiring access to mission networks are required by NASA to undergo a basic background check.[15]

SYSTEM AND SERVICE ACQUISITION	
Allocation of Resources (SA-02)	NIST: The organization: (a) Determines information security requirements for the information system or information system service in mission/business process planning; (b) determines, documents, and allocates the resources required to protect the information systems or information system service as part of its capital planning and investment control processes; and (c) establishes a discrete line item for information security in organizational programming and budgeting documentation. NIST supplemental guidance: Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service.
	Reality: Legacy missions/projects, that is, missions on extended life have minimum funding to continue their science operations. Unfortunately, the budget for these missions may not be enough to cover the expenses related to information technology.
	Tailoring recommendation/rationale: The tailoring of the control is for legacy missions only. Identify all controls that cannot be implemented by a limited-funded mission/project, and document the deviations in the SSP.

[15] National Agency Check with Inquiries (NAC-I)

System Development Life Cycle (SA-03)	NIST: The organization: (a) Manages the information system using [organization-defined system development life cycle] that incorporates information security considerations; (b) defines and documents information security roles and responsibilities throughout the system development life cycle; (c) identifies individuals having information security roles and responsibilities; and (d) integrates the organizational information security risk management process into system development life cycle activities. NIST supplemental guidance: A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. [..]
	Reality: Throughout the development phases of the mission, projects go through various milestone reviews which allow NASA to learn the development status of the various aspects of the project, and of course verify that the requirements for a specific milestone review are being satisfied. Current project milestone review requirements for IT security focus mostly on security documents. Projects/missions naturally place emphasis on security documentation, not necessarily on security processes (e.g., one-time vulnerability scans vs. continuous monitoring). While IT security documentation is a required necessity to support certain managed processes, the check-the-box review approach does not provide any benefit to the mission/project unless the core of the documentation, that is, the actual contents, is reviewed and scrutinized.
	Tailoring recommendation/rationale: In addition to meeting all project milestone review criteria, missions/projects should consider reporting on the status of other IT risk management processes as well.
Security Engineering Principles (SA-08)	NIST: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. NIST supplemental guidance: Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. [..]
	Reality: A&A is needed, and must be considered by design to avoid delays and additional costs down the road.
	Tailoring recommendation/rationale: Pay special attention to the organizational frequency of A&A so projects can budget accordingly.

PROGRAM MANAGEMENT	
Insider Threat Program (PM-12)	NIST: The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team. NIST supplemental guidance: Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. [..]

	Reality: By design, the ground system and mission operations architecture offer layered security, especially for protecting critical elements such as mission operations centers, but all these layers of security aim at protecting the ground system from external threats. Organizations supporting the ground system may not have a formal and mature insider threat program (unless the organization is supporting Department of Defense projects, in which case they are required to establish an insider threat program). This control is part of the Program Management (PM) control family which is not always addressed by individual elements.
	Tailoring recommendation/rationale: Organizations operating ground system elements should consider establishing an insider threat program to further protect the elements of the ground system. Comment: It might be possible to establish a ground system-wide insider threat program. If elements of the ground system do not have one in place, it may be more cost-effective to create one for the ground system in general.
Threat Awareness Program (PM-06)	NIST: The organization implements a threat awareness program that includes a cross-organization information-sharing capability. NIST supplemental guidance: Because of constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. [..]
	Reality: Current information security and privacy awareness training programs may address APTs, but only superficially.
	Tailoring recommendation/rationale: Consider establishing a threat awareness program, perhaps in conjunction with existing information security and privacy awareness training programs.

It is important to note that not all tailoring will be accepted or approved by the organization, especially when little or no organizational tolerance for deviations from standard (enterprise) implementation exists.

VI. Enterprise IT Security

Standardized IT solutions aim to be deployed in mass, covering as many divisions and departments as possible. The less customization and deviation from the standards the better and easier for the organization to verify implementation and compliance. As deployments are customized and tailored for certain environments, the organization must keep track of changes, and assume a different posture when assessing the tailored implementation. That is why there is often organizational resistance in permitting the customization of these deployments, including the selection, tailoring and scoping of the baseline security controls. One size does not fits all.

To date, FISMA attempted to apply baselined security controls across the federal government to standardize the management of information security. It took on a one size fits all approach, but gave agencies enough leeway to tailor the baselined controls so they better fit the business environments in which these agencies operate in. With the update to FISMA in 2014, the Federal Information Security Modernization Act (FISMA), an amendment to the 2002 Act, designated the Department of Homeland Security (DHS) the responsibility and authority to administer agency information security policies and practices. One of the outcomes from this update is the Continuous Diagnostics and Mitigation (CDM) program.

The CDM program being deployed across the federal government remains consistent with the one size fits all philosophy, and aims at the enterprise as a whole. Among the initiatives that are part of this program is the employment of automated tools to perform "periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents."[16] Highly specialized systems such as NASA's ground systems and mission operations are included under the CDM program, that is, are required to meet the requirements for the assessment and reporting of security (or lack thereof). Certainly, a thorough review of the security impact of the deployment of CDM sensors[17] on these highly specialized systems must be performed to prevent risks and/or impact to missions/projects. Over the years, missions/projects have developed internal processes to ensure that mission operations are not impacted by day-to-day IT management and IT security activities. The work that NASA does is sponsored by U.S. taxpayers, and as such, the Agency must be diligent in ensuring that the investment that it does on its missions is protected.

VII. Conclusion

Security audits are conducted not only to ensure that requirements are met (compliance verification) but also to identify problems, especially recurring problems, and their root causes so they can be prevented in the future. As we observe these recurring problems across multiple organizations, we the authors feel the professional responsibility to help the aeronautics and astronautics community address common issues affecting specifically the implementation and assessment of security controls. Most of these issues are caused by the improper selection of the security controls, in particular the lack of tailoring of the security controls to ensure that the controls fit the ground system (and mission operations) environment. By compiling a set of security controls based on their candidacy for tailoring into a single list, we believe we can assist current and future elements and organizations in (a) analyzing the applicability of security controls; (b) identifying deviations from the baselines; (c) identifying compensating controls for each deviation; and (d) document the tailored controls in the SSP. This list is not a recipe for customizing the baseline controls for the ground system, especially because each environment is unique. So unique it should not be treated the same as the rest of the enterprise. We hope we can provide insight to Information System Owners as they take this important step of the security life cycle.[18]

[16] Excerpt from the Federal Information Security Modernization Act of 2014, Public Law 113-283, 113th Congress [online], URL: https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf [retrieved 15 August 2016]

[17] CDM tools that collect information from devices, and report the information to a centralized report server (Federal Dashboard).

[18] NIST Risk Management Framework, NIST Cybersecurity Framework.

Appendix A: Acronyms

$(ISC)^2$	International Information System Security Certification Consortium
A&A	Assessment and Authorization
AC	Access Control (NIST 800-53 security control family)
ACSO	Alternate Computer Security Official
APT	Advanced Persistent Threat
AT	Awareness and Training (NIST 800-53 security control family)
ATO	Authorization To Operate
AU	Audit and Accountability (NIST 800-53 security control family)
BSU	Bowie State University
C&C	Command and Control
CA	Certification Authority
	Security Assessment and Authorization (NIST 800-53 security control family)
CCB	Change Control Board
CDM	Continuous Diagnostics and Mitigation
CISSP	Certified Information System Security Professional
CISTO	Computational and Information Sciences and Technology Office
CM	Configuration Management (NIST 800-53 security control family)
CP	Contingency Planning (NIST 800-53 security control family)
CPC	Climate Prediction Center
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
	Federal Information Security Modernization Act of 2014
FTP	File Transfer Protocol
GDMS	General Dynamics Mission Systems
GS	Ground System
GSFC	Goddard Space Flight Center
HSPD-12	Homeland Security Presidential Directive 12
IA	Identification and Authentication (NIST 800-53 security control family)
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IR	Incident Response (NIST 800-53 security control family)
IT	Information Technology
ITF	Instrument Team Facility
ISO	Information System Owner
ISSE	Information System Security Engineer
ISSO	Information System Security Officer
JHU	Johns Hopkins University
LACS	Logical Access Control System
LAN	Local Area Network
LDCM	Landsat Data Continuity Mission
MA	Maintenance (NIST 800-53 security control family)
MAVEN	Mars Atmosphere and Volatile EvolutioN
MMOC	Multi-Mission Operations Center
MO	Mission Operations
MOC	Mission Operations Center
MOE	Mission Operations Element
MP	Media Protection (NIST 800-53 security control family)
MU-SPIN	Minority University-SPace Interdisciplinary Network
NASA	National Aeronautics and Space Administration
NCEP	National Centers for Environmental Prediction
NIST	National Institutes of Standards and Technology

NOAA	National Oceanic and Atmospheric Administration
NPP	NPOESS Preparatory Project
ODV	Organization-Defined Value
OMB	Office of Management and Budget
OSIRIS-REx	Origins, Spectral Interpretation, Resource Identification, Security, Regolith Explorer
PACS	Physical Access Control System
PE	Physical and Environmental Protection (NIST 800-53 security control family)
PEAP	Protected Extensible Authentication Protocol
PIA	Privacy Impact Analysis
PIV	Personal Identification Verification
PL	Planning (NIST 800-53 security control family)
PM	Program Management (NIST 800-53 security control family)
	Project Manager
PS	Personnel Security (NIST 800-53 security control family)
RA	Risk Assessment (NIST 800-53 security control family)
RMF	Risk Management Framework
SA	System Administrator
	System and Services Acquisition (NIST 800-53 security control family)
SBU	Sensitive But Unclassified
SC	System and Communications Protection (NIST 800-53 security control family)
SCAP	Security Content Automation Protocol
SESDA	Sciences and Exploration Data Analysis
SI	System and Information Integrity (NIST 800-53 security control family)
SIA	Security Impact Analysis
SOC	Science Operations Center
SP	Special Publication
SSL	Secure Socket Layer
SSMO	Space Science Mission Operations
SSP	System Security Plan
TCP	Transfer Control Protocol
TESS	Transiting Exoplanet Survey Satellite
TLS	Transport Layer Security
UHF	Ultra High Frequency
UI	User Interface
US	United States
USB	Universal Serial Bus
USGCB	United States Government Configuration Baseline
VHF	Very High Frequency
WebUI	Web User Interface

Acknowledgments

The authors would like to thank Mr. Jeffrey Volosin (NASA/GSFC, TESS Project Manager (PM) and TESS ISO), for his support of the information security management work on the TESS mission as well as for supporting the development of this manuscript; Ms. Vickie Moran (NASA/GSFC, TESS Deputy PM) and Mr. Matthew Ritsko (NASA/GSFC Deputy PM for Resources) for their support of the information security management work on the TESS mission; Mr. Elmer "Sonny" Jones (GDMS, TESS GS Manager and GD Senior Staff for Greenbelt Programs); Mr. Fran Wasiak (GDMS, GD Deputy Manager for Greenbelt Programs); and Mr. H. Jackson Byrd III (GDMS, SSMO ISSE), for supporting the development of this manuscript.

References

[4] "The State of Cybersecurity from the Federal Cyber Executive Perspective," $(ISC)^2$ survey report [online], URL: https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/US_Government/ISC2-Federal-Cyber-Survey-Report.pdf [cited 07 August 2016].

[9] NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations [online], URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [cited 12 August 2016].

[10] NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach [online], URL: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf [cited 12 August 2016].

[11] NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations [online], URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [cited 12 August 2016].

[13] Takamura, E., Mangum, K., Wasiak, F., Gomez-Rosa, C., "Information Security Considerations for Protecting NASA Mission Operations Centers (MOCs)," 2015 IEEE Aerospace Conference [online], URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7119207 [cited 14 August 2016].

[15] Excerpt from the Federal Information Security Modernization Act of 2014, Public Law 113-283, 113th Congress [online], URL: https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf [retrieved 15 August 2016]

Author Biographies

Eduardo Takamura graduated cum laude with a B.S. in Computer Science from Bowie State University (BSU) in 1998, a M.S. in Computer Science from the Johns Hopkins University (JHU) in 2002, and became a Certified Information System Security Professional (CISSP) in 2008. He has been with NASA/GSFC for over 17 years having previously served as ISSO for the NASA Mars Atmosphere and Volatile EvolutioN (MAVEN) mission; ISSE for the Origins, Spectral Interpretation, Resource Identification, Security, Regolith Explorer (OSIRIS-REx) mission; IT Manager for the NASA Sciences and Exploration Data Analysis (SESDA) II program; Principal System Administrator for the NASA SESDA II, Minority University-SPace Interdisciplinary Network (MU-SPIN) education project as well as for the NOAA/NCEP Climate Prediction Center (CPC); and Alternate Computer Security Official (ACSO) for the NASA/GSFC Computational and Information Sciences and Technology Office (CISTO). As an undergraduate student, Eduardo worked on research projects at BSU and at the Georgia Institute of Technology (Georgia Tech). He is currently serving as ISSE for the Transiting Exoplanet Survey Satellite (TESS) mission, and supports the NASA Space Science Mission Operations (SSMO) project as Lead Vulnerability Assessor. Previously supported missions include the Landsat Data Continuity Mission (LDCM) Mission Operations Element (MOE), NPOESS Preparatory Project (NPP), and Glory. Eduardo authored the papers *"Information Security Considerations for Protecting NASA Mission Operations Centers (MOCs)"* and "*MAVEN Information Security Governance, Risk Management, and Compliance (GRC): Lessons Learned*" presented at the 2015 and 2014 IEEE Aerospace Conference respectively.

Kevin Mangum is a 2002 graduate from the University of Maryland University College with a Bachelor's of Science Degree in Technology Management. He has been with General Dynamics for 15 years and has supported various missions at NASA/GSFC for over 36 years. He has supervised system engineering groups for the development of near real time and level zero processing as well as management of operational teams. He has over 11 years of experience within the IT security environment, obtaining his Certified Information System Security Professional (CISSP) certification from $(ISC)^2$. Currently, he is supporting the Space Science Mission Operations (SSMO) missions in the role of the Information System Security Official (ISSO). Kevin co-authored the papers *"Information Security Considerations for Protecting NASA Mission Operations Centers (MOCs)"* and "*MAVEN Information Security Governance, Risk Management, and Compliance (GRC): Lessons Learned*" presented at the 2015 and 2014 IEEE Aerospace Conference respectively.