Information Security Considerations for Protecting NASA Mission Operations Centers (MOCs)

Eduardo Takamura, Kevin Mangum, Fran Wasiak
General Dynamics Mission Systems
Seabrook, MD USA

Carlos Gomez-Rosa
NASA/GSFC
Greenbelt, MD USA

Abstract—In NASA space flight missions, the Mission Operations Center (MOC) is often considered “the center of the (ground segment) universe,” at least by those involved with ground system operations. It is at and through the MOC that spacecraft is commanded and controlled, and science data is acquired. This critical element of the ground system must be protected to ensure the confidentiality, integrity and availability of the information and information systems supporting mission operations. This paper identifies and highlights key information security aspects affecting MOCs that should be taken into consideration when reviewing and/or implementing protecting measures in and around MOCs. It stresses the need for compliance with information security regulation and mandates, and the need for the reduction of IT security risks that can potentially have a negative impact to the mission if not addressed. This compilation of key security aspects was derived from numerous observations, findings, and issues discovered by IT security audits the authors have conducted on NASA mission operations centers in the past few years. It is not a recipe on how to secure MOCs, but rather an insight into key areas that must be secured to strengthen the MOC, and enable mission assurance. Most concepts and recommendations in the paper can be applied to non-NASA organizations as well. Finally, the paper emphasizes the importance of integrating information security into the MOC development life cycle as configuration, risk and other management processes are tailored to support the delicate environment in which mission operations take place.

Keywords—access control; asset protection; automation; change control; connection protection; continuous diagnostics and mitigation; continuous monitoring; ground segment; ground system; incident handling; information assurance; information security; information security leadership; information technology leadership; infrastructure protection; IT security metrics; least privilege; logical security; mission assurance; mission operations; mission operations center (MOC); NASA; network security; personnel screening; policies and procedures; physical security; risk management; scheduling restrictions; security controls; security hardening; software updates; system cloning and software licenses; system security; system security life cycle; unauthorized change detection; unauthorized change deterrence; unauthorized change prevention.

This paper was sponsored by NASA’s Mars Atmosphere and Volatile EvolutionO (MAVEN) Project based at Goddard Space Flight Center in Greenbelt, MD.

I. INTRODUCTION

The National Aeronautics and Space Administration (NASA), as every U.S. federal agency, is required by law to manage the security of its information systems. This includes implementing and maintaining a set of security controls to ensure the confidentiality, integrity and availability of information and information systems. With stagnant or even shrinking budgets, Agency projects struggle to meet minimum requirements for IT security. Missions often take a checklist approach to meeting minimum security requirements; one that does not always take risk reduction into consideration, but rather a compliance-driven approach to ensure the mission advances from one gated phase of the project life cycle to another. While compliance is necessary for missions to successfully “pass” these gates, and ultimately become operational, the goal is to reduce risks in order to increase security. Compliance alone does not assure security. Compliance efforts must be complemented by and governed with an effective IT risk management process. Both analytical and quantitative methodologies contribute to this reduction of risks, with emphasis on the mitigation of risks with greater impact to operations. In this paper, we propose to tackle these higher-impact risks first instead of sequentially implementing/auditing controls based on their checklist order.

We identify key security aspects that must have priority handling based on the impact to mission operations should they be mishandled or neglected. Finally, we look at potential roadblocks to the implementation of security controls for protecting mission operations centers, and how to overcome them.

A. Ground Systems and Mission Operations Overview

Mission operations are usually achieved through several ground systems that make up the ground segment for any NASA mission. At the core of any ground segment is the MOC. This is generally where command and control as well as health and safety monitoring of the spacecraft occur. The flight operations team, through their real-time command and

2 Also referred to the “C.I.A. triad.”
3 Throughout this paper, the term “Agency” and “NASA” are used interchangeably, and so are the terms “projects,” “organization” and “mission.”
4 See [1] for lessons learned in implementing and auditing governance, risk management, and compliance (GRC) throughout the development of NASA’s MAVEN mission to Mars.
control subsystem, and aided by trending, planning and other subsystems, operate the spacecraft. For typical science-based missions, a science operations center may also be employed. It is often a bridge between the scientists and the flight operations team where they handle the science operations of the mission. This can involve adjudicating science proposals, building the science plan and command sequences, and housing and distributing science data to the user community. To flow the information between the ground systems and to the spacecraft, networks are incorporated into the ground segment. For flight-to-ground communications, typical networks include the Space Network, the Near Earth Network, and the Deep Space Network. NASA’s Communications Service Office, formerly known as NASA Integrated Services Network, and the Jet Propulsion Laboratory mission network are two frequently utilized networks to tie ground systems together.

B. Compliance vs. Risk Reduction

Throughout the years, NASA projects including space flight missions have focused mostly and sometimes solely on compliance with federal regulations rather than on actual security threats. The pursuit of an information security Certification and Accreditation, or Security Assessment and Authorization in NASA lingo, at times, shifts the focus from reducing IT security risks to chasing IT security document required for obtaining an authorization to operate from the Agency. This authorization is given by the Authorizing Official, an executive official responsible for the entire information system, and is a product of the certification and accreditation (assessment and authorization) process.

While compliancy ensures that federal information systems meet minimum security requirements, the ultimate goal of security is to reduce risks. A cyber attacker is not concerned about whether the project has developed a system security plan according to an accepted template, and that the plan is in configuration control. The attacker is interested in finding out a way to breach the perimeter, compromise a system, and gain access to information and information resources.

As part of our auditing work, we must verify that a set of security controls have been successfully implemented by the mission, and are working as intended, in a manner that not only satisfied IT security requirements, but also ensures the confidentiality, integrity and availability of the mission information and information systems are protected. Such controls must also operate as intended.

There are 614 items (security controls, sub controls and control enhancements) in the National Institute of Standards and Technology (NIST) special publication 800-53 for moderate impact systems. Projects must not only focus on their missions, but they must also ensure that all applicable security requirements are met. For most projects – including space flight projects – these requirements include the 600+ security items that must be addressed as part of the security control selection step of the NIST Risk Management Framework [4] in addition to other requirements per organizational policy.

C. Scope and Applicability

This paper focuses on the security of NASA mission operations centers as part and in support of an overall ground segment. Many of the security considerations are applicable to elements external to the MOC, especially since the security of external elements may affect the security of the MOC. With the exception of the section on protecting connections, most external element security will be out-of-scope from this paper. The universal nature of the security aspects being addressed by this paper enables a broader adoption by non-NASA, non-government and even international entities responsible for protecting critical information systems, albeit critical infrastructure is out-of-scope. The target audience for this paper includes ground system managers, flight operations team managers, operators and support personnel; mission operations managers, information system owners, information system security officials, system and network administrators, MOC architects and integrators, and personnel responsible for the protection of critical facilities.

D. Disclaimer

The authors of this paper have performed numerous security assessments of NASA MOCs both at a NASA center and at NASA contractor facilities, and have been members of flight operations teams. At the time this paper was written, none of the authors was in the business of designing, building and/or operating MOCs.

While proven techniques exist, there is no recipe for handling risks since risk tolerance vary from project to project based on a variety of factors (e.g., applicability, available resources, existing protecting measures, environmental characteristics, exposure level, etc.). Each system (people, technology, processes, etc.) is unique. Risk analysis and mitigation require an understanding of the problem as well as an understanding of the environment that is subject to the problem. The recommendations provided herein are meant to provide supplemental guidance for evaluating the security of MOCs on top of existing standards and procedures for security assessments. They are not complete, they are not shortcuts to implementing security controls, and they should not replace any existing security checklist.

Fully observing the recommendations in this paper may not even ensure adequate protection of the MOC if existing organizational policy and procedures are not followed. Finally, there is never 100% security coverage or a 100% security guarantee.

II. APPROACH

When evaluating the security of the MOC, one must ask the following questions:

1. What are you protecting? (Sample answer: Data; information; information resources; etc.)
2. Why are you protecting? (Sample answer: Mission assurance; mission success)

---

5 See Access Control: Connection Protection.
3. *What or whom are you protecting from?* (Sample answer: Advanced persistent threats; costly mistakes; etc.)

4. *How and when can such protection fail?* (Sample answer: Through the successful exploitation of vulnerabilities in information systems after unauthorized access to information and information resources; human weaknesses (e.g., social engineering); procedural violations; single point of failures; etc.)

5. *What must be looked at to ensure protective measures remain strong and effective?* (Sample answer: Resource availability; processes and technology solutions; etc.)

While each MOC is unique, there are common security aspects that must be looked at when answering question 5 above. These security aspects are presented herein in the form of high-level security considerations, and may be evaluated during the MOC development and/or during the annual security assessment of the MOC. Ideally, these considerations are integrated into the development life cycle of the MOC.

We recommend the following approach: 1) Go over the security considerations presented in this paper to ensure critical security concerns are addressed by the MOC first; then 2) comply with institutional policies and applicable Federal laws and regulations (e.g., certification and accreditation). Projects must ensure that enough time is allocated to do both prior to scheduled security authorization.

Why go over the critical aspects first rather than implement security controls sequentially as they appear in a checklist? Certain security policies and management frameworks are designed to “fit all,” and they address concerns regarding programmatic, performance, and other issues that although are very important for operations, they may not address MOC vulnerabilities and other weak aspects that could be exploited by cyber attackers.

III. SECURITY CONSIDERATIONS

In this section, we will cover various security considerations that are highly recommended to be addressed by MOC architects, maintainers, and managers. These considerations are organized by groups:

- **Access Control**
- **Configuration Management**
- **Maintenance and Monitoring**
- **Management and Support**

Although these groups exist in NIST publication 800-53 as security control families⁶, they are highlighted herein to facilitate the identification of the areas that require most attention. These are not referring to the NIST security controls of the same name. A mapping of these groups against the NIST security controls as well as against the SANS critical security controls are given in Appendix B and C respectively.

IV. PART I – ACCESS CONTROL

A. **Access Control: Overview**

One of the top concerns in information security is the unauthorized access to information and information systems. Unauthorized access to the MOC, whether physically or logically, is unacceptable due to spacecraft commanding and controlling capability that MOCs possess. If successful in penetrating perimeter defenses, for example, a cyber-attacker may compromise one or more systems within the MOC, and take control of the spacecraft. Therefore, MOCs must ensure that access to its information and information systems is controlled and monitored, and any unauthorized access is detected and deterred.

In order to control access, it is necessary to identify what is being accessed, by whom, from where to where, when, how, how often, for how long, etc. We shall focus on three important managed resources that must be protected:

- **Assets**
  (e.g., computing devices, software, people, etc.)
- **Infrastructure**
  (e.g., facilities, network perimeter(s), networking devices, etc.)
- **Connectivity**
  (e.g., internal and external connections, link availability, etc.)

The least privilege principle⁷ must be applied and enforced by controlling access to information and information technology resources.

B. **Access Control: Asset Protection**

MOCs rely on information for mission operations. The confidentiality, integrity and availability of IT assets such as computing devices, software, people, etc. must be enable, enforced, and protected. All assets must be identified before they can be protected. Existing tools help automate the identification of new or modified assets on the network as well as removed or non-responding devices. This capability is particularly important to address “bring your own device (BYOD)” concerns. IT assets supporting mission operations include workstations, servers, firewalls, routers, switches, portable computing devices (if any), storage devices, software, etc. Each must be hardened for security, and properly configured to enforce access control (see Part II C. Configuration Management: Security Hardening below).

Various techniques for controlling/restricting access to systems and devices can be applied:

- System/application account restrictions (user accounts)
- Network access restrictions (whitelisting)

⁶ See Appendix B: Mapping Information Security Considerations to NIST Special Publication 800-53 Revision 4 Security Control Families.

⁷ Defined by NIST [8] as the authorization of user access (or processes acting on behalf of users) only to the extent “necessary to accomplish assigned tasks in accordance with organizational missions and business functions.”
C. Access Control: Infrastructure Protection

For both physical and logical security, MOCs must minimize the number of ports of entry into the MOC area and systems. The number of doors, windows, ventilation openings, etc. need to be identified and reduced to prevent unauthorized physical and/or visual access to information and information systems.

Many NASA missions do a good job in protecting the facilities that house the MOCs, and this paper will not expand on the topic other than list the following physical security items of interest:

- Key/card access by authorized users only
- Escorted visitor access
- Access log review
- Security cameras (if any)
- Guarded facilities
- Redundant power

Likewise, the number of network ports on the systems must be reduced to the minimum required for operations. Logical access to these “open” ports must be restricted to authorized users through firewalls and/or access control lists through whitelisting (allow specific, deny everyone else). Blacklisting (disallow specific, allow everyone else) may also be used, but only in conjunction with a whitelist.

Firewalls are often mistakenly regarded as the final and at times sole solution for protecting the network perimeter. The existence of a firewall alone does not indicate that the perimeter is protected. One must review the firewall rules and access control lists to ensure that only authorized objects/subjects are explicitly allowed to access information resources. Firewalls are only one of many security layers that must be applied not only to the MOC but also to all elements of the ground system.

Most MOCs do not require Internet access, and so the capability should not exist unless the mission has a valid justification for exposing the MOC systems to the open Internet. Examples of mission needs for Internet access include access to vendor patches; data transfers for backup/archival purposes; access to asset management servers; etc. Even so, there are alternatives to this access, for instance, the establishment of a single patch or mirror server local to the MOC that establishes the external connection to the vendor web sites, obtains the necessary software updates, and serves the MOC systems internally.

D. Access Control: Connection Protection

The link between the MOC and other interconnected elements must be protected against unauthorized access including tampering with the data in transit. In most cases, the information being transmitted to/from the MOC carries some level of sensitiveness, and must be protected accordingly. Encryption via Secure Shell (SSH) and/or Transport Layer Security (TLS) is often employed to protect the data, especially the credentials that are used for authentication.

In addition to encrypting the links external to the MOC, it is important to review all interconnections, and the relationship trust between the MOC and the external elements. Information on how data is protected on each end (i.e., at and by the MOC, and at and by the external element) is usually captured in interconnection security agreements between the two elements. From the MOC perspective, the security of interconnecting sites is important since they can be targeted by attackers with the intention of using them and their trusted relationship with the MOC to infiltrate the MOC (or just to hijack MOC input/output data).

V. Part II – Configuration Management

A. Configuration Management: Overview

In the past, some NASA missions could get away with a mission-issued mandate to freeze their ground system configuration, especially if they were expected to be short-lived and/or had reduced or no budget for information technology and information security maintenance and support. Examples of such a freeze include software updates, and hardware upgrades. Today many missions continue on way past their expected life span. FISMA, by design, places accountability on senior executives who own and are responsible for the risks related to non-implementation of required security controls.

B. Configuration Management: Change Control

To keep up with information technology it is necessary to handle changes in software and hardware without compromising the security of the information system. Controlling changes through a formal change management process can reduce risks by applying techniques to review the change and the risks incurred by the change, approving the change, testing the change, and finally making the change. And if the change still “breaks” the system, a rollback mechanism shall bring back the previous configuration.

The formal change management process must include IT security considerations – with a security official (or designee) sign-off – to ensure that security is considered as part of the change process.

C. Configuration Management: Security Hardening

Operating systems and applications are shipped with the general user in mind. By default, they are not configured for security. NASA MOCs, like any Agency system, must configure devices for security by applying standards-based, organization-provided security configuration settings to software. Benchmarks by the Center for Internet Security, vendor-recommended hardening guides, and other government-recommended security settings are some of the standards that can be applied to MOC systems.

8 Some projects are still using the now vulnerable Secure Sockets Layer (SSL) protocol.
The general rule of thumb (and NASA policy) is to apply all recommended settings that are applicable to the system, and document deviations from the standard with the reason why the setting was not applied.

D. Configuration Management: System Cloning and Licensing

A common configuration management practice employed by system administrators is system cloning. Once the system is configured for security (i.e., hardened), tested, and ready for placement into production, system administrators can save a snapshot of the system image as a system configuration baseline, and duplicated it as needed. This saves valuable time, and can prevent misconfiguration due to possible human errors. Software licensing and license restrictions, however, must be observed when performing these cloning operations to prevent software license violations. If a single license software is installed on the system that is cloned, the clone now contains a copy of the software. Unless allowed by the software vendor, the “user” should not make copies of the software. Most open software and freeware software do not impose such restrictions. For more considerations on software licenses, see Maintenance and Monitoring: Software Updates.

VI. PART III – MAINTENANCE AND MONITORING

A. Maintenance and Monitoring: Overview

Vulnerabilities in software are being discovered each day, and missions must keep up with the constant updates to software addressing the vulnerabilities.

Hardware maintenance is also important, from firmware updates to protection from environmental agents (e.g., electrical issues, humidity, dust/particle exposure, heat, etc.). Hardware security is often associated with physical and environmental security.

B. Maintenance and Monitoring: Software Updates

Out of the box, operating systems and applications may already contain vulnerabilities due to flawed software. The flaws (or software bugs) can be fixed by applying patches/updates to the vulnerable software. Due to the frequency of patches/updates released by vendors – at least monthly, in most cases – MOCs must follow an appropriate patch management process. This process must be coupled with other related processes such as configuration management, risk management, vulnerability management, and acquisitions to name a few.

MOCs (and information systems supporting the ground system in general) must take into consideration the restrictions imposed by critical mission events. For instance, a configuration freeze may be imposed on the element (i.e., the MOC) preventing system configuration modifications including those promoted by the patching or updating of the system.

Project and MOC management must consider continued software and hardware support throughout the life of the mission to ensure uninterrupted access to software updates (patches). This requires early planning by the Project to address this requirement. Unfortunately, many missions that enter extended life have to drop such support to remain extended. Even if support remains, the mission may dismiss project support personnel that would perform such functions as data management (e.g., backups), patch testing and deployment, system support, etc. Due to risks associated with untested patching, these missions opt to not deploy any patches at all.

One of the considerations that these legacy missions\(^9\) have is to mimic the system environment of the spacecraft when operating spacecraft simulation software. In this case, patching/updating their simulators will modify the configuration of the system; thus, affecting the integrity of the simulations. The mission decides not to patch/update these particular systems.

If risks related to flawed software cannot be mitigated, then compensating controls must be applied. For instance, systems that are and will not be patched should be air-gapped.

Note: Patching MOC systems to fix flawed software will not only address vulnerabilities with the software that could potentially be exploited for unauthorized access and/or disclosure of information, but may also correct issues pertaining to software and hardware performance (e.g., memory handling; new hardware support; etc.).

C. Maintenance and Monitoring: Unauthorized Change Prevention, Detection and Deterrence

Changes to systems, networks, etc. require technical and administrative controls. The change control consideration under configuration management above is an example of an administrative control to ensure that proposed changes are analyzed for risks; approved; tested; and deployed with the capability of rolling back to a previous configuration. This is fine for intentional changes by authorized personnel, but systems and networks must be configured to prevent, detect and deter unauthorized changes, either intentional or unintentional.

Unauthorized changes can be prevented by proper system configuration, that is, by the security hardening of the system. Successful and/or failed unauthorized changes are often detected by automated integrity checkers, and audit log analysis. The automatic deterrence of agents attempting or executing unauthorized changes is challenging since authorized users may mistakenly and/or unknowingly attempt to change protected system configuration.

D. Maintenance and Monitoring: Incident Handling

In security, it is no longer a matter of if your system will experience a security incident, but when. Being prepared for security incidents both intentional and unintentional might prevent further damages from incidents, and assist in security incident investigations. Security incidents may include hardware failures since the unavailability of information resources also constitute a violation of the confidentiality,

---

\(^9\) Missions on extended life.
integrity and availability triad. MOC personnel must be trained on identifying incidents, reporting them, and handling incidents according to policy.

E. Maintenance and Monitoring: Continuous Monitoring

MOCs must have a continuous monitoring plan in place and in execution to ensure that the security status of all assets, infrastructure devices, and connections is known and monitored on an on-going basis. The intent is to know the health and vulnerability state of IT resources in real- or near-real-time. System hardware state and software patch levels are two major monitored items to verify access and “aliveness” as well as to identify vulnerabilities, if any, due to flawed software.

The continuous monitoring process should be automated as much as possible. The use of Security Information and Event Management (SIEM) systems in connection with Intrusion Detection Systems (IDSes) can facilitate the monitoring of events by automating the detection and notification of suspicious activities, by facilitating the analysis of events, and by speeding up the response to security alerts.

VII. PART IV – MANAGEMENT AND SUPPORT

A. Management and Support: Overview

The management of IT and IT security in support of the MOC and the ground system in general is essential; however, in the eyes of cyber attackers, the low-hanging fruit that can facilitate the exploitation of vulnerabilities and ultimately enable them to break into the MOC is without any doubt technical and operational in nature. That is why this paper was organized to address access control, configuration management, and maintenance and monitoring first before addressing management and support considerations. True, IT and IT security policies define the security posture of an organization, and ensure that processes and procedures are followed in a standardized and expected manner, but hostiles will turn to configuration settings and vulnerabilities to break into networks and systems. Many of the management and administrative controls exist to ensure that processes are followed, and human errors are reduced or eliminated. Social engineering and deception may be utilized to gain insight into the organization or even open up a backdoor into the perimeter. Hence the need for not only a security-aware operations support personnel, but also for qualified and background-screened workforce supporting the MOC. Finally, time considerations ensure that certain resource-consuming IT activities are not scheduled at the same time as when a critical mission event occurs, and that MOCs deliver work products in time by key gated reviews.

B. Management and Support: Information Technology and Information Security Leadership

The information technology and information security realms are constantly evolving thus requiring proper management and support to reduce (IT) risks, and increase (IT) security. Information technology and information security leadership must understand the mission, and the environment in which the mission operates in.

The mission Information System Owner (ISO) is the person responsible for the acquisition, development, integration, operation, modification, maintenance, and disposal of information systems [5]. The ISO is familiar with the mission, and must understand his/her roles and responsibilities regarding the security of the information technology supporting the mission. The mission Information System Security Official (ISSO), the security advisor to the ISO, is someone who is knowledgeable of the organization’s security policies, processes and procedures. Together, both the ISO and the ISSO are stewards of security for the project, and indirectly protects the Agency.

The knowledge and the involvement of the ISO are of utmost importance to the project since the ISO will make certain risk decisions that can effectively define the security posture of the mission. A leader who does not engage in (IT) risk-based decisions and/or who lacks the knowledge of IT security requirements is definitely a risk to the mission.

The fact that some of the ISOs have control or influence of the mission’s budget can facilitate the risk mitigation process since there could be costs associated with risk mitigation. Also, there may be costs associated with security incidents, especially related to the cleaning up after a security incident.

Mission directors play an important leadership role in information security. Like the ISO, mission directors can and should count on the mission ISSO for information security recommendations, and ensure that the information security considerations documented in this paper are reviewed.

C. Management and Support: Personnel Screening

Because MOC personnel have access to information systems that provide them with indirect control of multi-million dollar spacecraft, minimum background security screening is necessary. Everyone with access to the MOC information systems should undergo a background investigation — such as the National Agency Check with Inquiries (NAC-I) – that can identify suspected behavior, past or present, that may be a threat to the MOC and the mission in general. The insider threat is a serious threat because of the privileges and permissions that the employee already has that could allow the employee to bypass controls meant to counter external attacks.

 Needless to say, IT personnel supporting the MOC have been given the “keys to the kingdom” to install, configure and maintain MOC IT resources. These professionals must possess appropriate technical knowledge and skills to perform such duties without violating policy and/or compromising the security of information and information systems.

D. Management and Support: Policies and Procedures

Most security assessors and assessment teams rely on a project’s existing security documentation to plan for security evaluations, and use it as reference to support the execution of the assessments. In fact, many projects place emphasis on security documentation since security work products can be
more easily quantified (i.e., counted) compared to services which are more qualitative. Documentation, when well-written, can provide the necessary guidance for smooth operations. Attackers, however, are not necessarily interested in the project’s security documents unless these documents can serve them with information that can facilitate an attack. Once again, compliance does not equate to security.

While not mandatory, an overall mission IT security management plan documenting how IT security is/will be managed and supported across the ground system, including the MOC, can be useful in evaluating how the MOC security will be assessed against mission requirements. Not to be confused with the MOC system security plan that documents specifically how the MOC is/will be secured.

E. Management and Support: Scheduling Restrictions

In mission operations, there are critical events that require special attention when scheduling IT and IT security activities. This includes the scheduling of IT maintenance activities such as the deployment of software updates (e.g., patches), security scanning (e.g., vulnerability scanning), etc.

Communications and communication processes must be established and in use to coordinate IT and IT security activities. Most missions utilize existing configuration management processes for coordinating events.


During the development of the MOC (and the ground system in general), the project must meet certain IT security requirements that are verified by NASA’s Independent Program Assessment Office (IPAO) [6] at different phases of the NASA project life cycle. Fig. 1 in Appendix A identifies such requirements per [5]. In addition, Table II also in Appendix A lists recommended IT security deliverables for each life cycle phase.

G. Management and Support: IT Security Metrics

How does one know whether applying these considerations to MOC design, development and/or operations can truly reduce risks to improve security of the MOC? As with most managed processes, the effectiveness of the processes can be determined by measuring performance, statistics, etc. before and after implementation of the (new) process(es), and continuously afterward. Metrics data to be captured will depend on what is to be measured. Some examples of security items to be measured include:

- Number of new {incidents | vulnerabilities (discovered) | Plan of Actions and Milestones (opened)} in the past 30 days;
- Number of open {incidents (i.e., under investigation) | vulnerabilities (not yet mitigated) | Plan of Actions and Milestones (not yet closed)} in the past 30 days;
- Number of closed {incident investigation(s) | vulnerabilities (mitigated) | Plan of Actions and Milestones} in the past 30 days.

Historical metrics data must be kept and used for trending analysis which can influence and even determine an appropriate course of action for the reduction of risks to information and information technology. This is accomplished via the POA&M process for risk mitigation or risk acceptance.

VIII. POTENTIAL ROADBLOCKS

Security assessments, like most audits and inspections, aim to identify issues to be corrected before problems occur. Despite the fact that such discovery and corrective actions can prevent security incidents, and therefore spare projects and organizations the cost of incident clean up, many missions may still face potential roadblocks when addressing or attempting to address the proposed security considerations. The following scenarios illustrate potential challenges MOCs can face, and possible responses to each one of them:

A. Lack of Information Technology/Security Leadership Support

Without a champion for IT and IT security at the management level, MOCs may struggle to implement required security controls, risking failure to attain an Authorization To Operate (ATO). One has the power and the responsibility to start with the MOC Manager, and keep escalating to the next higher position until senior leadership is aware of the lack of leadership support for IT and IT security. The Federal Information Security Management Act (FISMA) places responsibility and accountability for IT security on senior executives, and if IT security is not being diligently managed, proper channels must be notified (e.g., senior leadership, Contracting Officers including Contracting Officer Technical Representatives, etc.).

B. Lack of Managed Processes

Managed processes ensure a certain level of maturity in operations, especially with regard to configuration and risk management, resulting in more efficient outcomes with lower probability of errors, mistakes and mishaps. If managed processes are not in place, then IT and IT security activities will likely be impacted (e.g., delayed). If managed processes do not exist, any necessary process will need to be formalized. Standard procedures may help, initially and/or temporarily, but eventually a more solid methodology will be needed. Unfortunately, there are no effective workarounds for the lack of managed processes.

C. Lack of Qualified IT/IT Security Personnel

MOC IT operations require moderate to senior level technical support personnel. These professionals are expected to be knowledgeable and skilled not only in operating systems and applications, but also in configuration management, risk management (incl. vulnerability management), and in information security in general. If experienced technical

---


11 According to the organization’s data retention policy.
personnel are not available, training – including coaching/mentoring – may help offset for the lack of knowledge and skills to install, configure and maintain MOC systems.

Similarly, partner ground elements interfacing with the MOC may lack of necessary understanding of information security requirements, processes, etc. This issue should be brought up to both the ISO and the ISSO.

D. Tight Schedule

If the mission cannot afford to go through the information security considerations as grouped and prioritized in this paper, flip the sequence of the recommended approach so that compliance is addressed first. Missions must comply with IT security requirements in order to become and stay operational. When time permits, perhaps during and as part of annual security assessments, the mission may opt to audit the MOC per the security considerations presented here.

E. Lack of Funding

Some missions, especially those in extended life, may lack funding to support not only IT security activities but also IT activities in general such as maintenance and support of IT systems. It is particularly important for those legacy MOCs to focus on the Access Control and Configuration Management aspects of security since they will possibly be unable to address Maintenance and Monitoring, and Management and Support considerations.

F. MOC Location

If the MOC is located on non-government property (e.g., on commercial property), then there is a possibility that certain security controls may not satisfy Agency standards. A review of the controls is needed, and risk management processes must be followed to identify the risks associated with the controls, and the impact on the mission.

G. Contract Restrictions

If security requirements are not clearly defined, scoped and agreed upon in contracts between the Agency and service providers (contractors), then security requirements may not be met by the contractors. In this case, if the MOC is architected, developed and/or operated by contractors, the Agency may or may not be able to levy specific security requirements on the contractor(s).

IX. CONCLUSION

This paper identifies specific areas of concern that must be looked at before, during and after compliance checking assessments. It is meant to be used as a reference but not as a standard by those responsible for the security of mission operation centers. The goal is to ensure that key areas are inspected and fulfilled to make it difficult or even improbably for cyber attackers to break into the critical element of the ground system, ultimately reducing risks and increasing the security of the MOC.

For MOCs already implementing NIST SP 800-53 security controls, a mapping of the information security considerations to NIST security control families is listed in Appendix B. For MOCs already implementing the SANS Critical Security Controls, a mapping of the information security considerations to the SANS Critical Security Controls is presented in Appendix C. Finally, for MOCs already implementing ISO/IEC 27001:2013 controls, a mapping of the information security considerations to the ISO/IEC 27001:2013 controls can be found in Appendix D.

| Access Control | • Asset Protection  
| Configuration Management | • Change Control  
| Maintenance and Monitoring | • Software Updates  
| Management and Support | • Information Technology and Information Security Leadership  

Main takeaways:

- Know what you are protecting
- Know why you are protecting
- Know who you are protecting from
- Know how the protection can fail
- Know where to look at to make sure the protection does not fail
- Focus on key security aspects:
  - Access Control
  - Configuration Management
  - Maintenance and Monitoring
  - Management and Support
- Comply with organizational and applicable policy
- Look for potential roadblocks

U.S. Government work not protected by U.S. copyright.
X. APPENDIXES

Appendix A
NASA IT Project Life Cycle Phases, Key Decision Points, and Reviews

Fig. 1 above [7] shows the NASA IT project life cycle reviews and requirements per NASA Procedural Requirement 2810 [5] (highlighted). Table II below contains recommendations for key IT security processes and products to be delivered by each major review:

<table>
<thead>
<tr>
<th>TABLE II. RECOMMENDED DELIVERABLES BY PROJECT REVIEW</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mission Definition Review (MDR)</strong></td>
</tr>
<tr>
<td>System Requirements Review (SRR)</td>
</tr>
<tr>
<td>Recommendation:</td>
</tr>
<tr>
<td>• Requirements for IT security clearly defined and documented in Mission Information Technology Security Management Plan.</td>
</tr>
</tbody>
</table>

| **Preliminary Design Review (PDR)**  |
| Recommendation:  |
| • Initial selection of security controls applicable to the MOC.  |
| • Initial identification and documentation of interconnections, and preliminary Interconnection Security Agreements.  |
| • Preliminary MOC system security plan. |

| **Critical Design Review (CDR)**  |
| Recommendation:  |
| • Preliminary MOC Risk Assessment and MOC Risk Assessment Report based on the partial or non-implementation of security controls.  |
| • MOC (IT) Contingency Plan.  |
| • MOC Continuous Monitoring Plan  |
| • Desired:  |
|   • MOC (IT) Configuration Management Plan  |
|   • MOC (IT) Maintenance Plan  |
|   • MOC Plan of Actions and Milestones (POA&Ms)  |

| **Operational Readiness Review (ORR)**  |
| Recommendation:  |
| • Authorization To Operate (ATO)/Authorization To Process (ATP) 6 months prior to launch. |

U.S. Government work not protected by U.S. copyright.
Appendix B
Mapping Information Security Considerations to NIST Special Publication 800-53 Rev. 4 Security Control Families

The following table shows a mapping of the security consideration groups to the NIST special publication 800-53 security control “families”\(^\text{12}\).

<table>
<thead>
<tr>
<th>TABLE III. MAPPING INFORMATION SECURITY CONSIDERATIONS TO NIST SP 800-53 REV. 4 SECURITY CONTROL FAMILIES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Control</strong></td>
</tr>
<tr>
<td>• Access Control (AC)</td>
</tr>
<tr>
<td>• Awareness and Training (AT)</td>
</tr>
<tr>
<td>• Identification and Authorization (IA)</td>
</tr>
<tr>
<td>• Physical and Environmental Protection (PE)</td>
</tr>
<tr>
<td>• Personnel Security (PS)</td>
</tr>
<tr>
<td>• System and Information Integrity (SI)</td>
</tr>
<tr>
<td><strong>Configuration Management</strong></td>
</tr>
<tr>
<td>• Configuration Management (CM)</td>
</tr>
<tr>
<td>• Contingency Planning (CP)</td>
</tr>
<tr>
<td>• Planning (PL)</td>
</tr>
<tr>
<td>• System and Services Acquisition (SA)</td>
</tr>
<tr>
<td>• System and Information Integrity (SI)</td>
</tr>
<tr>
<td><strong>Maintenance and Monitoring</strong></td>
</tr>
<tr>
<td>• Audit and Accountability (AU)</td>
</tr>
<tr>
<td>• Security Assessment and Authorization (CA)</td>
</tr>
<tr>
<td>• Configuration Management (CM)</td>
</tr>
<tr>
<td>• Contingency Planning (CP)</td>
</tr>
<tr>
<td>• Incident Response (IR)</td>
</tr>
<tr>
<td>• Maintenance (MA)</td>
</tr>
<tr>
<td>• Media Protection (MP)</td>
</tr>
<tr>
<td>• Physical and Environmental Protection (PE)</td>
</tr>
<tr>
<td>• Risk Assessment (RA)</td>
</tr>
<tr>
<td>• System and Services Acquisition (SA)</td>
</tr>
<tr>
<td>• System and Information Integrity (SI)</td>
</tr>
<tr>
<td><strong>Management and Support</strong></td>
</tr>
<tr>
<td>• Planning (PL)</td>
</tr>
<tr>
<td>• Personnel Security (PS)</td>
</tr>
<tr>
<td>(All of the Program Management (PM) controls as applicable: Information Security Program Plan (PM-1); Senior Information Security Officer (PM-2); Information Security Resources (PM-3); Plan of Action and Milestones Process (PM-4); Information System Inventory (PM-5); Information Security Measures of Performance (PM-6); Enterprise Architecture (PM-7); Critical Infrastructure Plan (PM-8); Risk Management Strategy (PM-9); Security Authorization Process (PM-10); Mission/Business Process Definition (PM-11); Insider Threat Program (PM-12); Information Security Workforce (PM-13); Testing, Training, and Monitoring (PM-14); Contacts with Security Groups and Associations (PM-15); Threat Awareness Program (PM-16)).</td>
</tr>
</tbody>
</table>

\(^\text{12}\) For a description of each control family, see [8] (p.2).
### Appendix C

Mapping Information Security Considerations to SANS Critical Security Controls [9]

<table>
<thead>
<tr>
<th>TABLE IV.</th>
<th>MAPPING INFORMATION SECURITY CONSIDERATIONS TO SANS CRITICAL SECURITY CONTROLS</th>
</tr>
</thead>
</table>
| **Access Control** | • Asset management (A.8)  
• Access control (A.9)  
• Cryptography (A.10)  
• Physical and environmental security (A.11)  
• Communications security (A.13)  
• Information security aspects of business continuity management (A.17) |
| **Configuration Management** | • Asset management (A.8)  
• Cryptography (A.10)  
• Physical and environmental security (A.11)  
• System acquisition, development and maintenance (A.14)  
• Supplier relationships (A.15)  
• Information security aspects of business continuity management (A.17) |
| **Maintenance and Monitoring** | • Asset management (A.8)  
• Physical and environmental security (A.11)  
• Operations security (A.12)  
• System acquisition, development and maintenance (A.14)  
• Supplier relationships (A.15)  
• Information security incident management (A.16)  
• Information security aspects of business continuity management (A.17) |
| **Management and Support** | • Information security policies (A.5)  
• Organization of information security (A.6)  
• Human resource security (A.7)  
• Asset management (A.8)  
• System acquisition, development and maintenance (A.14)  
• Supplier relationships (A.15)  
• Information security incident management (A.16)  
• Information security aspects of business continuity management (A.17)  
• Compliance, with internal requirements, such as policies, and with external requirements, such as laws (A.18) |
### Appendix D

**Mapping Information Security Considerations to ISO/IEC 27001:2013 Controls**

<table>
<thead>
<tr>
<th>TABLE V.</th>
<th>MAPPING INFORMATION SECURITY CONSIDERATIONS TO ISO/IEC 27001:2013 CONTROLS</th>
</tr>
</thead>
</table>

| Access Control | • Inventory of Authorized and Unauthorized Devices (CSC 1) |
|                | • Inventory of Authorized and Unauthorized Software (CSC 2) |
|                | • Malware Defenses (CSC 5) |
|                | • Wireless Access Control (CSC 7) |
|                | • Security Skills Assessment and Appropriate Training to Fill Gaps (CSC 9) |
|                | • Secure Configurations for Network Devices such as Firewalls, Routers, and Switches (CSC 10) |
|                | • Limitation and Control of Network Ports, Protocols, and Services (CSC 11) |
|                | • Controlled Use of Administrative Privileges (CSC 12) |
|                | • Boundary Defense (CSC 13) |
|                | • Controlled Access Based on the Need to Know (CSC 15) |
|                | • Account Monitoring and Control (CSC 16) |
|                | • Data Protection (CSC 17) |
|                | • Secure Network Engineering (CSC 19) |

| Configuration Management | • Inventory of Authorized and Unauthorized Devices (CSC 1) |
|                         | • Inventory of Authorized and Unauthorized Software (CSC 2) |
|                         | • Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers (CSC 3) |
|                         | • Continuous Vulnerability Assessment and Remediation (CSC 4) |
|                         | • Application Software Security (CSC 6) |
|                         | • Wireless Access Control (CSC 7) |
|                         | • Data Recovery Capability (CSC 8) |
|                         | • Secure Configurations for Network Devices such as Firewalls, Routers, and Switches (CSC 10) |
|                         | • Limitation and Control of Network Ports, Protocols, and Services (CSC 11) |
|                         | • Controlled Use of Administrative Privileges (CSC 12) |
|                         | • Boundary Defense (CSC 13) |
|                         | • Controlled Access Based on the Need to Know (CSC 15) |
|                         | • Data Protection (CSC 17) |
|                         | • Secure Network Engineering (CSC 19) |

| Maintenance and Monitoring | • Continuous Vulnerability Assessment and Remediation (CSC 4) |
|                           | • Application Software Security (CSC 6) |
|                           | • Boundary Defense (CSC 13) |
|                           | • Maintenance, Monitoring, and Analysis of Audit Logs (CSC 14) |
|                           | • Account Monitoring and Control (CSC 16) |
|                           | • Data Protection (CSC 17) |
|                           | • Incident Response and Management (CSC 18) |
|                           | • Penetration Tests and Red Team Exercises (CSC 20) |

| Management and Support | • Security Skills Assessment and Appropriate Training to Fill Gaps (CSC 9) |

[10, Tab. A-1] offers a useful matrix mapping a set of controls identified by the CCSDS as most applicable to space systems, ground operations systems, and development facilities for spacecraft or ground systems; and grouped according to their related ISO 27001 subject areas.

[8, Tab. H-1 (in appendix H)] contains a mapping of NIST SP 800-53 security controls to ISO/IEA 27001.
ACKNOWLEDGMENT

The authors would like to thank the support from the NASA Mars Atmosphere and Volatile EvolutioN (MAVEN) mission leadership for understanding the requirements for IT security as applicable to the mission and its ground system, and for valuing the protection and consequently the reduced (IT) risks through effective information security governance, risk management, and compliance. Throughout the development and operational phases of the MAVEN mission, many of the security considerations presented in this paper were applied to the MAVEN MOC. The auditing work for the NASA Space Science Mission Operations (SSMO) project including risk and vulnerability assessments of SSMO MOCs also provided valuable insights into the security considerations presented in this paper. Last but not least, we thank everyone who peer reviewed this paper, and who provided insightful comments and suggestions for improving this paper.

REFERENCES


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 16 years having previously served as UNIX/Linux System Administrator for the NASA Minority University-Space Interdisciplinary Network (MU-SPIN) education project as well as for the NOAA/NCEP Climate Prediction Center (CPC); Alternate Computer Security Official (ACSO) for the NASA/GSFC Computational and Information Sciences and Technology Office (CISTO); IT Manager for the NASA Sciences and Exploration Data Analysis (SESDA) II program; and IT Security Engineer/Auditor for the Landsat Data Continuity Mission (LDCM) Mission Operations Element (MOE), and NPOESS Preparatory Project (NPP). As an undergraduate student, Eduardo worked on research projects at BSU and at the Georgia Institute of Technology (Georgia Tech). Eduardo is currently serving the Mars Atmosphere and Volatile EvolutioN (MAVEN) mission as Information System Security Official (ISSO); the Transiting Exoplanet Survey Satellite (TESS) mission as Information System Security Engineer (ISSE); and the Space Science Mission Operations (SSMO) as Vulnerability Assessment Auditor. Eduardo authored the paper “MAVEN Information Security Governance, Risk Management, and Compliance (GRC): Lessons Learned” presented at the 2014 IEEE Aerospace Conference.

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 the General Dynamics C4S Corporation for 15 years and has supported various missions at NASA/GSFC for over 35 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 10 years of experience within the IT security environment, obtaining his Certified Information System Security Professional (CISSP)

U.S. Government work not protected by U.S. copyright.


Fran Wasiak received a B.S. in Mechanical Engineering from the State University of New York (SUNY) at Buffalo in 1989. His career started in the Mission Operations Directorate at the Johnson Space Center as a Payload Operations Engineer for the Space Shuttle Small Payloads Program and Lead Instrument Operations Engineer for both the National Oceanic and Atmospheric Administration's Polar Orbiting Environmental Satellites (POES) program and the NASA Earth Observing System (EOS) Aqua Program. Currently, Fran is the Lead Ground Segment Engineer for the NASA James Webb Space Telescope (JWST) and is the Deputy Mission Operations Manager for the Mars Atmosphere and Volatile Evolution (MAVEN) mission. Fran has authored papers on the topic of JWST Integration and Test for SPIE and SpaceOps conferences. Fran co-authored the paper “MAVEN Information Security Governance, Risk Management, and Compliance (GRC): Lessons Learned” presented at the 2014 IEEE Aerospace Conference.