

Space Segment Information Assurance Guidance for Mission Success

June 10, 2011

Frank C. Belz
Computers and Software Division
Engineering and Technology Group

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

Contract No. FA8802-09-C-0001

Authorized by: Space Systems Group

Developed in conjunction with Government and Industry contributions as part of the U.S. Space Programs Mission Assurance Improvement workshop.

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

Space Segment Information Assurance Guidance for Mission Success

June 10, 2011

Frank C. Belz
Computers and Software Division
Engineering and Technology Group

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

Contract No. FA8802-09-C-0001

Authorized by: Space Systems Group

Developed in conjunction with Government and Industry contributions as part of the U.S. Space Programs Mission Assurance Improvement workshop.

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

Space Segment Information Assurance Guidance for Mission Success

June 10, 2011

Frank C. Belz
Computers and Software Division
Engineering and Technology Group

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

Contract No. FA8802-09-C-0001

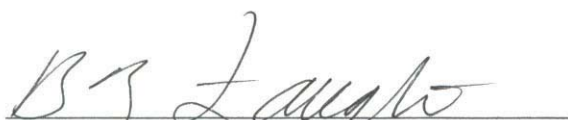
Authorized by: Space Systems Group

Developed in conjunction with Government and Industry contributions as part of the U.S. Space Programs Mission Assurance Improvement workshop.

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

Space Segment Information Assurance Guidance for Mission Success

Approved by:



B. Zane Faught, General Manager
Computers and Software Division
Engineering and Technology Group



Malina M. Hills, General Manager
MILSATCOM Division
Space Programs Operations
Space Systems Group

Acknowledgments

This document has been produced as a collaborative effort of the Mission Assurance Improvement workshop. The forum was organized to enhance Mission Assurance processes and supporting disciplines through collaboration between industry and government across the US Space Program community utilizing an issues-based approach. The approach is to engage the appropriate subject matter experts to share best practices across the community in order to produce valuable Mission Assurance guidance documentation.

The document was created by multiple authors throughout the government and the aerospace industry. We thank the following contributing authors for making this collaborative effort possible:

Craig C. Carter (Northrop Grumman Information Systems)
Faris Faris (Northrop Grumman Aerospace Systems)
Ron Kravetz (Space and Missile Systems Center (SMC))
Jim Mapes (Lockheed Martin Corporation)
John Norman (General Dynamics)
Wende Peters (Johns Hopkins University Applied Physics Laboratory)
Vance Saunders (Ball Aerospace & Technologies Corp.)
Brenda Taylor (The Aerospace Corporation)
Louisa Thomson (The Boeing Company)
Rex Tsou (Lockheed Martin Corporation)
Bill Walker (Ball Aerospace & Technologies Corp.)

A special thank you for co-leading this team and efforts to ensure completeness and quality of this document goes to:

Craig C. Carter (Northrop Grumman Information Systems)
Frank Belz (The Aerospace Corporation)

The Topic Team would like to acknowledge the support, contributions and feedback from the following organizations:

The Aerospace Corporation
Ball Aerospace & Technologies Corp
The Boeing Company
General Dynamics
Johns Hopkins University Applied Physics Laboratory
Lockheed Martin Corporation
Northrop Grumman Aerospace Systems
Northrop Grumman Information Systems
Orbital Sciences Corporation
Pratt & Whitney Rocketdyne (PWR)
Raytheon Space and Airborne Systems
Space and Missile Systems Center (SMC)

The authors deeply appreciate the contributions of the subject matter experts who reviewed the document:

Peter Suk (The Boeing Company)

Michael Phillips (Lockheed Martin Corporation)

Mark Stephenson, Francis Afinidad (Northrop Grumman Aerospace Systems)

Kendall Nii (Orbital Sciences Corporation)

Chris den Heijer (Pratt & Whitney Rocketdyne [PWR])

Carolyn Boettcher (Raytheon Space and Airborne Systems)

Contents

Executive Summary	xi
1. Introduction	1
1.1 Scope of this Guide	2
1.1.1 What it covers.....	2
1.1.2 What it doesn't cover.....	3
1.1.3 Space Segment of National Space Systems.....	3
1.1.4 Conventional Information Assurance Methods	3
1.1.5 Going Beyond Conventional IA Methods to Achieve Mission Resilience	6
1.2 Use of this Guide	7
1.3 Organization of this Guide	9
1.3.1 Chapter 1. Introduction.....	9
1.3.2 Chapter 2. Reference Material.....	9
1.3.3 Chapter 3. Applicable Governance, Standards, and Guidance	9
1.3.4 Chapter 4. Establishing a Cyber Mission Assurance Framework	9
1.3.5 Chapter 5. National Space System Acquisition Guidance.....	10
1.3.6 Chapter 6. National Space System Update and Development Guidance	10
1.3.7 Chapter 7. National Space Segment Operations Guidance	11
1.3.8 Chapter 8. Unresolved Challenges/Future Work.....	11
1.3.9 Appendix A. Risk Management Framework – Primer	11
1.3.10 Appendix B. Guideline Cross-Reference Matrix.....	11
2. Reference Material	13
2.1 Relevant / Referenced Documents	13
2.1.1 Government Policies, Directives, Instructions, and Reports	13
2.1.2 Technical Operating Reports from The Aerospace Corporation.....	21
2.2 Definitions	22
2.3 Acronym List.....	25
3. Applicable Governance, Standards, Guidance	29
3.1 Context: Past, Present, and Future.....	29
3.1.1 Past	30
3.1.2 Present – Harmonization and Transformation in Progress	32
3.1.3 Future Expectations	37
3.2 Common Governance and Risk Management Framework Are Not Enough	37

4.	Establishing a Cyber Mission Assurance Framework	39
4.1	Information Assurance/Cyber Security <i>Enablers</i> for Mission Assurance	40
4.1.1	Mission-Driven Assessment	41
4.1.2	Access Understanding/Control	42
4.1.3	Instrumentation/Measurement/Trust.....	43
4.2	Information Assurance/Cyber Security <i>Application Areas</i> for Mission Assurance.....	44
4.3	Information Assurance/Cyber Security <i>Participants</i> for Mission Assurance	45
4.4	Integrated Framework for Cyber Mission Assurance in Space Systems	45
4.5	Guidance	47
5.	National Space System Acquisition Guidance.....	53
5.1	Trends in National Space Acquisition.....	53
5.2	National Space Segment Acquisition Roles and Responsibilities	54
5.3	Programmatic Guidance.....	55
5.3.1	Guidelines	56
5.4	Acquisition Relationship to Governance and Standards Guidance.....	59
5.5	Acquisition Relationship to Cyber Mission Assurance Framework Guidance.....	59
6.	National Space System Update & Development Guidance	61
6.1	General Guidance.....	61
6.1.1	NSS-S Information Assurance Systems Engineering	62
6.1.2	NSS-S Ground Enclave Mission Assurance	63
6.2	Addressing the Advanced Cyber Threat for NSS-Space Components	64
6.2.1	Agility	64
6.2.2	System Hardening	67
6.2.3	System Monitoring.....	72
6.3	Cyber Hardening for the Space Segment.....	73
6.3.1	Enhanced Program Protection.....	73
6.3.2	Developing Mission Resilience	75
6.3.3	Program Architecture.....	81
6.3.4	Program Software Development	82
6.3.5	Program Hardware Development.....	84
6.4	Prioritizing Development Activities with Constrained Resources.....	86
7.	National Space Segment Operations Guidance.....	89
7.1	Improving space system space segment operations	89

7.1.1	Interface and Connectivity Identification, Documentation, and Enforcement	90
7.1.2	Configuration Management/Control of Space IT Assets.....	92
7.1.3	Authentication and Access Management/Administration	92
7.1.4	Consistent Enforceable Standards for Sustainment/Operational System Administration	94
7.1.5	Intrusion Detection, Audit, Prevention, and Eradication.....	94
7.1.6	Space Segment Change Management.....	95
7.1.7	Changing Threat, Vulnerability and Mitigation Profiles	96
7.1.8	Cyber Situation Awareness	97
7.1.9	Cyber Response Capability Enhancement.....	98
7.2	Protecting Space Programs in Operations	99
8.	Unresolved Challenges/Future Work	101
Appendix A.	Risk Management Framework – Primer	103
Step 1.	Security Categorization	103
Step 2.	Security Control Selection.....	104
Step 3.	Control Implementation	105
Step 4.	Control Testing and Assessment	105
Step 5.	Authorization.....	105
Step 6.	Continuous Monitoring	105
Appendix B.	Guideline Cross-Reference Matrix	107

Guidelines

Guideline 3-1. Be Cognizant of NSS IA Guidance Changes.....	37
Guideline 4-1. Perform Mission-Driven Analysis to determine mission-information dependencies.....	48
Guideline 4-2. Establish and Implement Access Control functions across system lifecycle.....	49
Guideline 4-4. Require Mission-based Cyber Situational Awareness.....	51
Guideline 4-5. Require Mission-based Cyber Course of Action Development.....	52
Guideline 5-1. Initiate enhanced Program Protection.....	56
Guideline 5-2. National Space Program IA Integrated Product Team (IPT).....	57
Guideline 5-3. IA Risk Management Integration in Program Milestones.....	58
Guideline 5-4. New Capability Insertion on Existing Programs.....	59
Guideline 6-1. Allocate IA requirements, goals and objectives down to components.....	63
Guideline 6-2. Provide technical capability to continuously secure all ground enclave interconnects.....	64
Guideline 6-3. Incorporate safe mode for space-borne processing subsystems.....	65
Guideline 6-4. Protect the safe mode from unauthorized activation.....	66
Guideline 6-5. Protect full and partial space segment operational software and database upload capability.....	67
Guideline 6-6. Document and maintain the system security architecture.....	68
Guideline 6-7. Policy monitoring and third party analysis to ensure security policy compliance.....	69
Guideline 6-8. Protect all space segment security boundaries, document risk and mitigate uncontrolled boundaries.....	70
Guideline 6-9. Ensure robust program protection for flight SW components.....	71
Guideline 6-10. Provide system subversion analysis and test.....	72
Guideline 6-11. Exploit standard telemetry streams for cyber situational awareness.....	73
Guideline 6-12. Periodically identify critical program information, technology and components.....	74
Guideline 6-14. Architectural trades for resilient mission-information exchanges to drive Mission Risk Management Approach.....	76
Guideline 6-15. Derive and implement system requirements to support operational access control.....	77
Guideline 6-16. Derive and implement system requirements from system resilience architecture and trust profiles.....	78
Guideline 6-17. Derive and implement IA component cyber event instrumentation requirements.....	79
Guideline 6-18. Provide Mission-based Cyber Situational Awareness display.....	80
Guideline 6-19. Derive technical requirements in support of Cyber Course of Action.....	81
Guideline 6-20. Protect the NSS-S Network in its entirety.....	82
Guideline 6-21. Implement robust SW and development processes.....	83
Guideline 6-22. Implement enhanced SW robustness for mission critical information objects per the NSA IASRD (OBJ).....	84
Guideline 6-23. Implement robust hardware and computing platforms.....	85
Guideline 6-24. Implement enhanced HW assurance for protection of mission critical information per the NSA IASRD (OBJ).....	86

Guideline 6-25. Incorporate Cyber-Security approach into the System Security Management Plan	87
Guideline 7-1. Document, maintain, and enforce the system security architecture over the system’s operational lifetime.....	91
Guideline 7-2. Develop and maintain a comprehensive System Configuration Management process	92
Guideline 7-3. Verify and maintain authentication compliance for fielded systems.....	93
Guideline 7-4. Develop and maintain enforceable standards for administration of fielded systems	94
Guideline 7-5. Implement appropriate intrusion detection and audit capabilities.....	95
Guideline 7-6. Implement patch management plan.....	96
Guideline 7-7. Conduct periodic threat, vulnerability, and mitigation reassessments	97
Guideline 7-8. Establish and maintain continuous Cyber Situation Awareness	98
Guideline 7-9. Refresh Cyber Response Capabilities	99
Guideline 7-10. Implement enhanced Program Protection Planning during operations	100

Figures

Figure 1-1. Tabular format for guidelines.....	3
Figure 1-1. Space Segment of National Space systems.	4
Figure 1-2. General acquisition and operations lifecycle.....	5
Figure 3-1. DIACAP security lifecycle.....	34
Figure 3-2. Risk management framework security lifecycle.	34
Figure 3-3. Alignment of DIACAP with risk management framework.....	36
Figure 3-4. Areas targeted for harmonization.	36
Figure 4-1. Preparing for a cyber-ready mission assurance framework.	40
Figure 4-2. Extending existing approaches to handle dynamic cyber environment.	41
Figure 4-1. Cyber mission assurance must span lifecycle.	44
Figure A-1. Risk management framework security lifecycle.	103

Tables

Table 2-1. Policies, Directives, Instructions, and Reports	13
Table 2-2. TORs.....	21
Table 3-1. Area- and Agency-Specific IA Guidance Examples	30
Table 3-2. Foundational Governance Policies and Standards.....	32
Table 3-1. Governance Selection/Applicability Criteria.....	33
Table 3-4. Publication Status of Foundational NIST Harmonization Documents	35
Table 4-1. Cyber Mission Assurance Framework Components	46
Table B-1. Guideline Cross-Reference from Sections 3-7 to Sections 3-5, 7.....	107
Table B-2. Guideline Cross-Reference from Sections 3, 5, 7 to Section 6.....	108

Executive Summary

Especially over the last two decades, the government and private sectors of the U.S. have come to a heightened awareness of the challenges to national security that are emerging by way of Cyberspace. These challenges bring into question the resilience of all the functions of our economy and government, including those of the military and intelligence communities, in the face of Cyberspace attacks and other threats.

This is a very dynamic time for all systems operating in Cyberspace, and particularly for National Space systems. In the midst of this flux, this guide is an attempt to frame the implications of the need to defend against and operate through attacks in Cyberspace, and where appropriate, capture some of the most critical and effective elements of Information Assurance (IA) that, when implemented, constitute best practices that can profitably be employed in new National Space system acquisition. It applies across the entire lifecycle of National Space systems, spanning the initial analysis that precedes the actual procurement of such systems; the initial development of new systems; the upgrade of existing legacy or heritage systems; and the operation of all National Space systems.

This guide describes existing governance, guidance, and standards in the area of Information Assurance, as applied to National Space systems, and describes how all three – governance, guidance and standards – are in flux. The guide also provides a mission assurance context in which the role of IA techniques can best be understood, and addresses what must be done to go beyond the conventional techniques of IA if true mission resilience is to be achieved.

The central chapters of the guide provide explicit guidance for the acquisition, development, update, and operation of National Space systems, focusing specifically on the Space Segment of those systems, as defined herein – the notion of the Space Segment is expanded somewhat beyond typical usage. The guide adapts IA guidance primarily developed for conventional ground-based information systems, focusing that guidance on the ability of the Space Segments of National Space systems to support mission resilience in an actively contested Cyberspace environment. Since the means for achieving both information assurance and mission assurance for the Space Segment of National Space systems are in such flux in the highly dynamic domain of Cyberspace, the guide also identifies some areas where unresolved challenges remain and future work will be required.

Guidance is in the form of specific recommendations, which are contained in numbered guidelines set apart in a tabular format. Guideline tables also provide additional useful information elaborating on why the recommendation is given, when the recommendation pertains (in the lifecycle), who would need to be involved in implementing the recommendation, and how they would know whether they are successfully following the recommendation.

Guidelines provided herein are not standards or policies, nor are they requirements. They define norms for stakeholders in National Space programs; certain norms may also apply to civil and commercial Space programs. They offer advice to stakeholders about what it means to implement the recommendations. In many cases, they reflect existing IA governance.

This guide is designed for:

- The government acquisition community/program offices to review and choose recommendations to implement
- Contractors to review and use recommendations to improve processes and command media
- Operations organizations to review and use recommendations to improve operational procedures and security practices

1. Introduction

The government and private sectors of the U.S. have come to a heightened awareness of the challenges to national security that are emerging by way of Cyberspace, especially over the last two decades. These challenges bring into question the resilience of all the functions of our economy and government, including those of the military and intelligence communities, in the face of Cyberspace attacks and other threats.

Although increasing attention is now being paid at all levels of government to meeting the challenges in Cyberspace, being aware of the challenges is a far cry from being able to meet them. Fortunately, the problem is not new. In fact, the nature of the problem has been recognized for decades by a small community of security experts. These experts have developed a substantial body of knowledge about how to protect and defend information technology (IT) systems so that mission-critical information is available in its proper and correct condition only to those who are entitled to it, when they need it. This body of knowledge, including the practices it encompasses, is generally designated as *Information Assurance (IA)*.

Implementing and applying IA techniques is not free, nor are the techniques themselves always easy to live with. These realities have often resulted in decisions not to employ them. Decisions have been made to ignore or defer applying many IA techniques at every level: by individual citizens who own personal computers, by program managers developing important information systems, and by corporate IT organizations responsible for providing their companies with Cyberspace services. Consequently, significant loss has been realized at all these levels: personal and corporate intellectual property and other mission critical information has been lost or stolen, information services have been disrupted, and delivery of products and services has been delayed, all due to successful Cyber intrusions/attacks.

Increased public awareness has stimulated not only increased interest in the techniques of IA, but also increased willingness to consider instituting those techniques to improve system operational resilience in the presence of Cyber threats. Within the defense and intelligence communities, a substantial body of IA policies, processes, standards, and technologies has been developed and is being mandated in the development of new systems and in the operation of fielded systems.

But the existence of the IA mandates does not necessarily mean that they can or will be executed expeditiously. The incorporation of IA techniques in fielded military and intelligence systems, and new systems under development, has been slow and has not been uniformly successful. Extensive IA governance policies and guidance documents are in place and are beginning to be applied to large ground information technology systems that are associated with satellite systems in National Security Space (NSS-S)¹ and National Civil Space programs (collectively termed “National Space” programs herein). But inconsistencies among these policies and documents impede their consistent application to the development and operations of these systems. Until recently, the satellites themselves have been considered sufficiently isolated that IA policies and guidance have been considered unnecessary for space vehicles and their payloads. That view has officially changed, and mandates for applying IA techniques in space have been instituted. But practice is slow to catch up to policy.

Instituting IA practices will certainly help to raise the bar against adversaries, making it more difficult and costly to achieve successful cyber attacks on National Space systems. Unfortunately, the awareness of the need to apply these practices has risen just as (and arguably *because*) the threat environment has become much stronger, more vital and more dynamic. It is part of the nature of much of Cyberspace that attacks are much easier to achieve than defense against those attacks, and this reality has become quite obvious in

¹ In this Guide, National Security Space is considered a contraction of National Security Systems – Space, so the acronyms NSS-S and NSS-Space are also used to refer to National Security Space.

recent years. Several studies, such as two recent studies by the Air Force Scientific Advisory Board, have concluded that it is no longer reasonable to believe that IA techniques will be completely effective in preventing successful Cyber attacks. Therefore, these studies conclude, we need to add to our attention on protection and defense of information and information systems (the traditional province of IA) a new emphasis on the resilience of the missions those systems serve. Even if our information systems are disrupted, degraded, or even partially destroyed by cyber attacks, how can the mission persist – how can those conducting the mission “fight through” the attacks? And for National Space, how can mission operators “operate through” the attacks? The shift is from sole attention to the narrower *system* (or even System of systems) concerns of Information Assurance to the broader *mission* concerns encompassed by Mission Assurance (MA). From this point of view, IA remains necessary but not sufficient to the success of National Space missions.

This is a very dynamic time for all systems operating in Cyberspace, and particularly for National Space systems. In the midst of this flux, this report is an attempt to frame the implications of the need to “fight/operate through” attacks in Cyberspace, and where appropriate, capture some of the most critical and effective elements of IA that, when implemented, constitute best practices that can profitably be employed in new National Space system acquisition, in the upgrade/development of existing “legacy” or “heritage” National Space systems, and in the operation of all National Space systems.

1.1 Scope of this Guide

1.1.1 What it covers

This Guide describes existing governance, guidance, and standards in the area of Information Assurance, as applied to National Space systems, and describes how all three – governance, guidance and standards – are in flux. The Guide also provides a mission assurance context in which the role of IA techniques can best be understood, and addresses what must be done to go beyond the conventional techniques of IA if true mission resilience is to be achieved.

The heart of the Guide provides explicit guidance for the acquisition, development and update, and operation of National Space systems focusing specifically on the Space Segment of those systems, as defined in section 1.1.3 (where the notion of the Space Segment is expanded beyond typical usage). Here the guide adapts IA guidance primarily developed for conventional ground-based information systems, focusing that guidance on the ability of the Space Segments of National Space systems to support mission resilience in an actively contested Cyberspace environment. Since the means for achieving both information assurance and mission assurance for National Space Systems Space Segment are in such flux in the highly dynamic domain of Cyberspace, the Guide also identifies some areas where unresolved challenges remain and future work will be required.

Guidance is in the form of specific recommendations, which are contained in numbered “Guidelines” set apart in a tabular format. Guideline tables also provide additional useful information elaborating on why the recommendation is given, when the recommendation pertains (in the lifecycle), who would need to be involved in implementing the recommendation, and how they would know whether they are successfully following the recommendation. Guideline tables follow the format given in Figure 1-1.

Note that guidance provided here is just that; guidelines are not requirements, nor are they standards, nor are they policies. They are instead simply judgments about specific activities that should be made throughout the lifecycle of the Space Segment of National Space System in order to improve the likelihood that the missions they serve will be better served in the presence of threats and adverse events/actions in Cyberspace. However, it is true that many of the guidelines here do encompass individual or multiple standard IA “controls” captured in documents such as DODI 8500.2 or NIST SP 800-53.

Guideline <#>: Title
Recommendation: <i>Summary description of the guidance.</i>
Evaluation Criteria: <i>Indication of ways in which one would be able to tell whether a guideline is being followed or has been achieved.</i>
Milestone: <i>Indication of the acquisition development and operations lifecycle phase(s) or milestone(s) in which the guideline is to be implemented.</i>
Rationale: <i>Reason the guideline is provided. May be expressed in a positive light, identifying the benefits of following the guideline, and/or in a negative light, identifying the consequences or potential consequences of failing to follow the guideline.</i>
Stakeholders/Actions: <i>Enumeration of stakeholders and the actions they must take to comply with the guidance.</i>

Figure 1-1. Tabular format for guidelines.

Much of the verbiage in this document falls outside the guidelines tables; this descriptive text is all intended to be informative, providing additional context, motivation, and examples pertinent to the guidance recommendations themselves.

1.1.2 What it doesn't cover

This Guide incorporates a broader than usual definition of the “Space Segment” of space systems in Section 1.1.3, but it does *not* go beyond that definition. It does not, for example, include mission data processing functions on the ground. For the most part, it considers National Space Systems developed for the sole use of the national security and civil space communities, rather than systems that are entirely or partially for use in the commercial world.

1.1.3 Space Segment of National Space Systems

For the purpose of this document, the Space Segment of National Space systems is defined as the Space Vehicle and its payloads; up/down/cross links; tracking, telemetry, and control (TT&C) communications and other on-ground functions required to control the SV and payload, and satellite interfaces in user equipment. Figure 1-2 is a schematic contextual representation of this definition, where all the parts of the Space Segment are depicted or labeled in yellow. This is somewhat more inclusive than other common usages of the term Space Segment, in order that the cyber-security specific issues that are pertinent to the successful functioning of space vehicles and their payloads can be addressed cleanly.

1.1.4 Conventional Information Assurance Methods

Information Assurance can be narrowly defined as those “measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.”² Information Assurance ensures that accurate

² CNSSI 4009, 26 April 2010.

information¹ is shared with and only with those authorized to access it², and is available when it is needed³.

In this document, the term IA has a somewhat broader meaning, referring to the body of knowledge and a set of practices that encompass such measures, for the purpose of contributing to mission assurance by developing information systems that can prevent, detect and (more recently) respond to disruptions or attacks, whether intended or not, while ensuring that critical information, systems, and services are not compromised, and countering the cyber threats throughout the lifecycle of the information, system, or service⁴. Note that this usage emphasizes the role of systems that are developed and operated in support of missions. IA typically focuses on these systems.

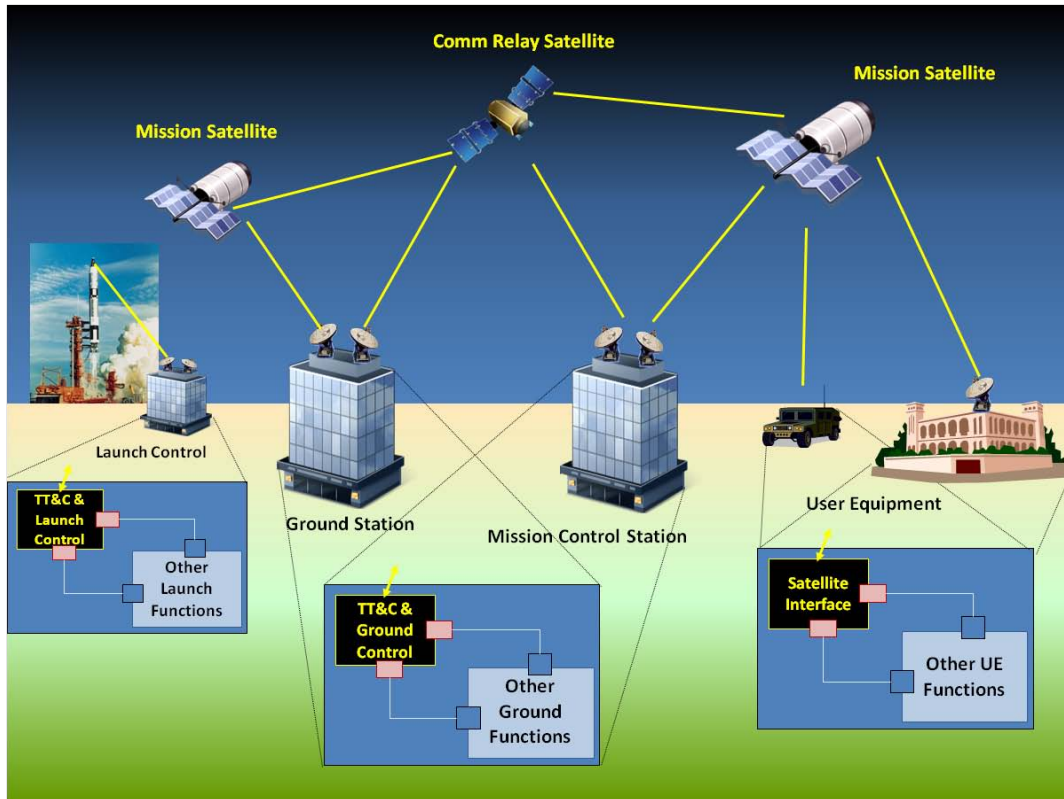


Figure 1-1. Space Segment of National Space systems.

The practice of IA is largely concentrated on the acquisition and operations cycle for such systems, and ideally is conducted in accordance with a discipline known as Information System Security Engineering (ISSE), also sometimes referred to as Information Assurance System Engineering (IASE). The acquisition and operations cycle is described somewhat differently across the DOD, Intelligence, and Civil Space communities, but the differences can be abstracted away in a generic depiction such as that of Figure 1-3⁵.

¹ Information that has not undergone unauthorized modification or destruction. Cf., definition of “Integrity”, Section 2.2.

² Cf., definition of “Confidentiality”, Section 2.2

³ Cf., definition of “Availability”, Section 2.2

⁴ Adapted from TOR-2010(8506)-7, Information Assurance: An Integral Component of Mission Assurance, as updated in the IA chapter of the most recent Mission Assurance Guide (MAG), TOR-2007(8546)-6018, REV A.

⁵ Adapted from NIST SP 800-64 Rev. 2.

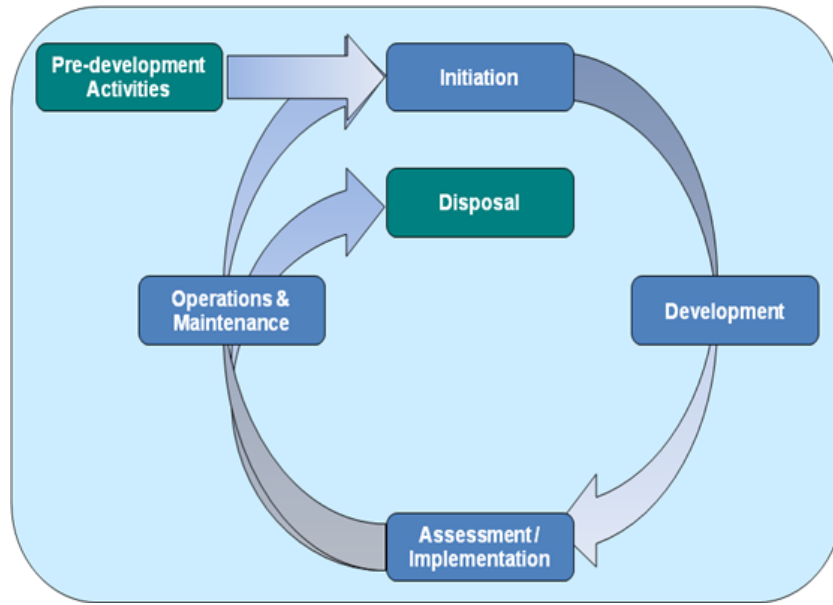


Figure 1-2. General acquisition and operations lifecycle.

In this depiction, the blue boxes represent the “internal” phases (generally called the System Development Lifecycle (SDLC)); the green boxes represent the starting and ending phases of the acquisition and operations lifecycle.

- Pre-development activities include the analyses contributing to the decision as to whether or not to develop a system to support a given mission or families of missions.
- Initiation activities include the analyses leading to determination of requirements for the system (or upgrades to it) and establishment of resources for and constraints upon the development of the system (or upgrades to it).
- Development activities include the definition and management of risk for the development of the system, the actual construction of the system (or upgrades to it), and the development testing of the system (upgrades) to determine the extent to which the system satisfies its requirements.
- Assessment/Implementation activities include the assessment of risk in the deployment and operation of the system as required to decide whether to deploy (for Space Segment system, launch) the system, as well as the actual deployment, initial configuration and check out (operational testing) of the system.
- Operations and Maintenance activities include conduct of the mission using the system, and the definition of improvements to the system to be conducted in subsequent full or partial iterations of the internal phases of the SDLC. During this phase, analysis of risks associated with ceasing to use the system, and a decision to decommission/dispose of the system may be made.
- Disposal activities include activities that may be required to minimize any residual risks associated with decommission/termination/disposal of the system.

The bulk of IA activities are conducted in the internal phases of the SDLC, starting with ensuring that an appropriate IA requirement set for the anticipated threat environment is captured in the system requirements documents and concept of operations. The majority of IA requirements are derived from federal or national-level laws, policies, directives, and instructions that are interpreted and supplemented

at the DOD or DNI level and at lower organizational levels⁸. These derived IA requirements are supplemented (or sometimes modified with appropriate approvals) with mission- and system-unique IA requirements that are derived from the system's required mission capabilities; concept of operations; intended operational environment and users; system threat assessment report (STAR) or equivalent; and other considerations. The process continues throughout the system lifecycle as IA concerns are integrated into the regular requirements feedback process, ensuring that systems are engineered, operated, and maintained to continually meet their IA requirements⁹. Many conventional IA activities required for Space Programs are described in TOR-2010(8506)-7, Information Assurance: An Integral Component of Mission Assurance, as updated in the IA chapter of the most recent Mission Assurance Guide (MAG), TOR-2007(8546)-6018, REV A.

All phases of the SDLC are rich with guidance and requirements for IA, both for the upgrade of existing systems and particularly for the development of new systems. Chapter 3 addresses the fact that multiple customer communities have evolved substantial, but distinct, sets of policies, standards, and guidance, which now are being harmonized in a major "transformation" process.

These IA requirements, as commonly implemented, provide a necessary baseline for securing systems against cyber attack, but are generally insufficient to provide mission resilience against the advanced cyber threat. IA requirements that are commonly implemented well among the National Space community are not repeated in this Guide, although selected requirements are provided when they lead to needed enhancements to common practice. In addition, this Guide provides more detailed guidance to achieve mission resilience as described in Chapter 4.

A specific conventional IA activity late in the SDLC is the subject of particular attention. In the Assessment/Implementation SDLC phase, the Certification and Accreditation (C&A) process culminates with the determination of whether "Authority to Operate (ATO)" is to be granted, enabling the system to be deployed. The decision to provide an ATO is risk based: an authorizing official (AO), external to the government program office for the system being developed, determines whether the risk to be incurred by system deployment can be tolerated in order to gain the benefit of that deployment. (In the DOD, this official is called the Designated Approval Authority or DAA.) If the authorizing official deems the risks acceptable, an ATO or Interim ATO (IATO) is granted. Ideally, the authorizing official has been involved in system security decisions throughout the SDLC so that the achievement of successful C&A does not become a stumbling block. In practice that often does not happen, and C&A is a major challenge for programs late in their pre-deployment process.

1.1.5 Going Beyond Conventional IA Methods to Achieve Mission Resilience

Highly resilient organizations recognize that, despite all planning and preparation, things do not go as anyone may have assumed; that the unexpected, if it is unprepared for, is as much an enemy of successful achievement of the organizational mission as any other factor; and that little vulnerabilities can be detected and fixed *before* an unanticipated major confluence of vulnerabilities, exploited by accident or adversarial intent, brings the mission to a halt.

⁸ The Defense Information Systems Agency (DISA) maintains a website (<http://iase.disa.mil>) that serves as a portal to IA policies, instructions, guidance, training, subject matter areas, tools, vulnerability information, and other references relevant to DOD missions. The Committee on National Security Systems (CNSS) maintains a website (<http://www.cnss.gov>) that serves as a portal to IA policies, instructions, guidance, training, subject matter areas, tools, vulnerability information, and other references relevant to the intelligence community.

⁹ Adapted from TOR-2010(8506)-7, Information Assurance: An Integral Component of Mission Assurance, as updated in the IA chapter of the most recent Mission Assurance Guide (MAG), TOR-2007(8546)-6018, REV A.

Preparation for, and thwarting of, adversarial actions in Cyberspace that can undermine information availability, confidentiality and integrity (and thereby mission assurance) is much of what IA is about. But when a space system has been deployed, and is in active operation, many small things will inevitably go wrong with aspects of the system or its use that weaken the effectiveness of the IA mechanisms and practices. Many of these instances will be identified as problems and fixed, because tactics, techniques and procedures (TTPs) demand it. But some will not. And sometimes the root causes of the things that go wrong will not be sought out and will not be fixed. An aphorism describing the effect of these events goes something like this: “The apex of system security is achieved shortly after C&A, just after ATO has been granted from the AO. After that, system security steadily declines.”

The tendency toward loss of security and resilience is *not unique* to space system operations. They apply in the most resilient of systems in use by the most resilient of organizations, as well as in the most brittle. The key factors that distinguish the highly resilient organizations are a culture and behavior that negate these effects, instituting a continual practice that:

1. Tracks and addresses small failures
2. Resists oversimplification that hides failures and vulnerabilities
3. Remains sensitive to the actual operational situation
4. Maintains capabilities for and commitment to resilience
5. Takes advantage of the expertise where it exists and applies that expertise where needed.¹⁰

For National Space Systems, the focus on these concerns goes beyond conventional IA to include issues that might be termed Cyber Mission Assurance. This term emphasizes that Mission Assurance requires direct attention to the challenge of “operating/fighting through” cyber attacks, even successful ones, to achieve critical mission objectives. This attention introduces substantial additions to the conventional System-focused IA techniques.

To a limited extent, this Guide addresses the practices required for Cyber Mission Assurance, using a framework presented in chapter 4. Furthermore, ongoing attempts to harmonize critical IA policies, standards and guidance as described in chapter 3 are moving away from a simple system-based approach to a mission-based approach. However, to address the aspects of the Cyber Mission Assurance framework defined in chapter 4 will require practices that go beyond the harmonization efforts of Chapter 3.

For all kinds of systems, and especially for National Space Systems, these practices are still not well understood. So not all guidance herein will be directed to these concerns, and it should be expected that in future years a great deal more experience dealing with these concerns will need to be captured in an updated or extended version of this Guide.

1.2 Use of this Guide

This Guide is designed for use by a spectrum of mission and system stakeholders. It provides a substantial body of descriptive information that would be of value to any participants in the National Space community. The guidance information in the Guide is designed first and foremost for government Program Office personnel and for those who directly support government Program Offices, such as FFRDCs and SETA contractors. For the most part, accepting and acting upon the guidance herein is up to government Program Office personnel. In addition, to follow the individual guidelines requires the involvement of a set of stakeholders that generally will go well beyond the government Program Offices.

¹⁰ Weick and Sutcliffe, *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*, 2nd Edition, Jossey Bass, 2007.

Here is a list of the stakeholder roles identified in this Guide whose involvement is essential to the adoption and execution of one or more of the guidelines.

- Overseeing Organization (Acquisition, Operations) – governmental organizations that are responsible for Program Offices and/or mission/system operations facilities.
- Government Program Office – government procurement agency for development of new functionality or systems, responsible to ensure all needed functionality is provided
- FFRDC – A Federally Funded Research and Development Center conducts research for the United States Government. They are administered in accordance with U.S Code of Federal Regulations, Title 48, Part 35, Section 35.017 by universities and corporations. FFRDCs work closely with the government's own staff members.
- UARC – A University Affiliated Research Center (UARC) is a strategic United States Department of Defense (DOD) research center associated with a university. UARCs often work closely with the government's own staff members
- SETA contractor – Systems Engineering and Technical Assistance (SETA) contractors are civilian employees or government contractors who are contracted to assist government acquisition programs. SETA contractors provide analysis and engineering services in a consulting capacity. They work closely with the government's own engineering staff members.
- User Segment, including both the System user, and the user equipment.
 - System (end) user - user of the system functionality. The system user's input should be sought for implementation of requirements that impact the end user's experience or interactions with the system (e.g., for NSS-S systems a consumer of sensor information or user of a satellite communications terminal).
 - User equipment – the portion of the National Space System that is in the possession of/used by the System user.
- System operator – personnel who maintain, administer and operate system equipment to enable it to provide functionality to system users (e.g., satellite or network operations personnel).
- System Network Operator – Network operations personnel who maintain, administer, and operate networks that are part of or interface with the system.
- Cyber personnel – personnel who maintain, administer, and operate those elements of system equipment that provide or reside in Cyberspace.
- Developer (software, hardware, firmware, subsystem) responsible for producing (developing, implementing, integrating, testing, and delivering) the Space Segment system and its elements.
 - Prime Contractor – Developer that has a direct contract with the government and whose work is overseen by the government Program Office.
 - Subcontractor – Developer that has a direct contract with the Prime Contractor or another subcontractor, and whose work is overseen directly or indirectly by the Prime Contractor and the government Program Office
 - Vendor – Provider of system components (software, hardware, firmware, subsystem) that are included in the system; these components are generally not developed uniquely/specifically for the system and are usually provided as commodity products.
 - Integrator – Developer that composes separate system components (Software, Hardware, Firmware, Subsystem) that, when composed, form the Space Segment system or one or more subsystems of the system.
- Tester/Evaluator – performs tests, evaluates systems either as part of the Developer community, the acquisition community, or as a third party.

- Security Organization (national, overseeing, program/operations) – National Security Organizations include, for example, the National Security Agency (NSA). Overseeing Organization Security Organizations have security responsibilities that span the program offices/operational facilities the overseeing organization is responsible for. Program/Operations security organizations are responsible for the security of systems being developed/operated, respectively.
- Authorizing Official (AO) – In DOD, the Designated Approval Authority (DAA) – government official with the ultimate responsibility of providing or withholding the system’s authority to operate (ATO). The AO is responsible for reviewing certification artifacts and making a risk assessment prior to allowing, or disallowing system operations. By providing an ATO, the AO formally assumes responsibility for operating a system, asserting that such operation will be at an acceptable level of risk. The AO is generically responsible for the adequacy of security controls.
- Certification Authority (CA) – senior official having the authority and responsibility for the certification of information systems governed by a component IA program, certified IA components and controls will be part of the larger system to be approved by the AO.

1.3 Organization of this Guide

The chapters of this Guide are enumerated here, and for each chapter, the relevance of the chapter to specific stakeholder roles is identified.

1.3.1 Chapter 1. Introduction

Chapter 1 introduces the Guide. This chapter is pertinent to all stakeholders.

1.3.2 Chapter 2. Reference Material

Chapter 2 provides reference material: lists of (i) documents, (ii) definitions of key terms, and (iii) acronyms used throughout this report. This chapter is pertinent to all stakeholders.

1.3.3 Chapter 3. Applicable Governance, Standards, and Guidance

Chapter 3 focuses on conventional IA methods, and discusses recognized standards, governance, and guidance that must be considered when developing new or supporting operational or legacy space systems. This chapter provides (1) a brief historical overview of IA practices within the federal government and associated difficulties and challenges, (2) current IA practices with respect to the space segment, and (3) convergent and transformative activities that are currently taking place to establish ubiquitous IA standards across the federal government.

Government Program Offices are responsible for determining whether or not to implement the guideline provided in this chapter.

In addition, these Program Offices are responsible for executing the actions implied by the guideline, although they may (contractually) delegate the actions to supporting players in one or more of these roles: FFRDC, UARC, SETA contractor or developer.

1.3.4 Chapter 4. Establishing a Cyber Mission Assurance Framework

Chapter 4 addresses going beyond conventional IA methods to achieve mission resilience through a Cyber Mission Assurance Framework. It provides an over-arching Mission Assurance view of Information Assurance elements; addresses the IA enablers and application areas for Mission Assurance;

identifies Cyber Mission Assurance participants and how they interact; and provides guidance on how to move National Space Systems toward being able to achieve the degree of resilience required for mission success.

It should be noted that the guidance in chapter 4 is generally extremely ambitious, often exceeding what is understood to be achievable today, or going beyond what is affordable (in cost and time). Chapter 8 addresses some topics that are motivated by chapter 4 guidelines but are not thought to be reasonably implementable today.

On the other hand, many guidelines in chapters 5, 6, and 7 are derived from chapter 4 guidelines, and those guidelines are thought to be implementable, at least to some degree, within reasonable cost and schedule constraints.

Government Program Offices are responsible for determining whether or not, and to what degree, to implement the guidelines provided in this chapter. In most cases, decisions on chapter 4 guidelines will not be made directly, but will be reflected in the determination of which guidelines in chapters 5, 6 and 7 are to be implemented and the degree to which they are implemented.

Execution of the guidelines in this chapter may require players in one or more of these roles: Program Office (including FFRDC, UARC, SETA), system user, system operator, developer, integrator, tester/evaluator, system network operator, and Cyber personnel.

1.3.5 Chapter 5. National Space System Acquisition Guidance

Chapter 5 provides specific guidance on the overarching acquisition/programmatic processes before, during, and after development and deployment of the Space Segment of National Space systems.

Government Program Offices are responsible for determining whether or not to implement the guidelines provided in this chapter.

Execution of the guidelines in this chapter may require players in one or more of these roles: Acquisition organization, Program Office (including FFRDC, UARC, SETA), system user, system operator, developer, integrator, National Security Organization, and AO.

1.3.6 Chapter 6. National Space System Update and Development Guidance

Chapter 6 provides specific guidance on the system development and system upgrade processes for the Space Segment of National Space systems.

Government Program Offices are responsible for determining whether or not to implement the guidelines provided in this chapter.

Execution of the guidelines in this chapter may require players in one or more of these roles:

- Program Office (including FFRDC, UARC, SETA)
- system user
- system operator
- S/W, H/W, System developer (prime, subcontractor, vendor)
- integrator
- AO
- CA

1.3.7 Chapter 7. National Space Segment Operations Guidance

Chapter 7 provides specific guidance on the operation of the Space Segment of National Space Systems.

Operations oversight organizations are responsible for determining whether or not to implement the guidelines provided in this chapter.

Execution of the guidelines in this chapter may require players in one or more of these roles: Operations oversight organizations/Program Office (including FFRDC, UARC, SETA), system operator, system user, National Security Organization.

1.3.8 Chapter 8. Unresolved Challenges/Future Work

Chapter 8 lists some of the unresolved challenges and candidates for future work. The guidance captured in the other chapters of this Guide should improve the ability of those in charge of National Space Systems to “fight/operate through” attacks in Cyberspace. It reflects what is known today about meeting that need. As more is learned about how to meet that need, we expect additional MAIW efforts to capture best practices that will emerge and that will be validated in upcoming years. This chapter identifies some of the areas where we expect to see improvements in the future.

1.3.9 Appendix A. Risk Management Framework – Primer

Appendix A provides a terse overview of the Risk Management Framework.

1.3.10 Appendix B. Guideline Cross-Reference Matrix

Appendix B provides a matrix describing relationships among the guidelines provided in Chapters 4 through 7.

2. Reference Material

2.1 Relevant / Referenced Documents

The following documents are referenced herein, or are relevant to the discussions and guidance herein.

2.1.1 Government Policies, Directives, Instructions, and Reports

Table 2-1. Policies, Directives, Instructions, and Reports

Document ID	Title & Location	Scope & Applicability
AFI 33-200	Air Force Instruction 33-200: Communications and Information, Information Assurance (IA) Management (Last revision 15 October 2010) http://www.e-publishing.af.mil/shared/media/epubs/AFI33-200.pdf ¹¹	Instruction. Provides general guidance for implementing IA and managing IA programs. Detailed guidance exists in reference documents such as DODI 8500.2. “Applies to ISs owned, operated, or supported by the AF including components of weapons systems”
CNSSI 1253	Security Categorization And Control Selection For National Security Systems (October 2009) http://www.cnss.gov/Assets/pdf/CNSSI-1253.pdf	Instruction. Provides the process for selecting baseline security and programmatic controls in Appendix F&G of NIST SP 800-53, and how to implement those controls. “Applies to all federal government departments, agencies, bureaus, and offices that collect, generate, process, store, display, transmit, or receive National Security Information.”
CNSSI 4009	National Information Assurance Glossary (26 April 2010) http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	Instruction. Resolves differences between the definitions of terms used by the DOD, IC and Civil Agencies to enable all three to use the same glossary (and move towards shared documents and processes). Applies to “all U.S. Government (USG) Departments, Agencies, Bureaus and Offices; supporting contractors and agents; that collect, generate, process, store, display, transmit or receive classified or sensitive information or that operate, use or connect to NSS.”

¹¹ All references to Worldwide Web URLs are accurate as of 1 March 2011.

Document ID	Title & Location	Scope & Applicability
CNSSP 12	National Information Assurance Policy For Space Systems Used To Support National Security Missions (20 March 2007) http://www.cnss.gov/Assets/pdf/CNSSP-12.pdf	Policy. Ensures the success of national security missions that use space systems by fully integrating IA into the planning, development, design, launch sustained operations and deactivation of those space systems used to collect, generate, process, store, display, or transmit national security information, as well as any supporting or related national security systems. Applies to “all space system launched, owned, operated, controlled, and leased by the USG, or for the benefit of the USG by commercial entities (either domestic or foreign/international and foreign governments).”
CNSSP 22	Information Assurance Risk Management Policy for National Security Systems (February 2009) http://www.cnss.gov/Assets/pdf/CNSSP-22.pdf	Policy. Establishes the requirements for enterprise IA risk management within the national security community and provides a framework for decision makers to continuously evaluate and prioritize IA risks in order to accept or recommend strategies to remediate or mitigate those risks to an acceptable level. “Applies to all federal government departments, agencies, bureaus, and offices including their supporting contractors and agents, that operate, use, or manage national security systems.”
DCID 6/3	Manual – Protecting Sensitive Compartmented Information Within Information Systems (5 June 1999)	Rescinded by ICD 503
DODI 8510.01	DOD Information Assurance Certification and Accreditation Process (DIACAP) (28 November 2007) http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf	Instruction. Establishes a C&A process to manage the implementation of IA capabilities and services and provide visibility of accreditation decisions regarding the operation of DOD ISs including core enterprise services-and Web services-based software systems and applications. Applies to “DOD-owned ISs and DOD-controlled ISs operated by a contractor or other entity on behalf of the Department of Defense that receive, process, store, display, or transmit DOD information, regardless of classification or sensitivity.”
DOD 5220.22-M	National Industrial Security Program Operating Manual (28 February 2006) http://www.dss.mil/isp/odaa/documents/nispom2006-5220.pdf	Operating Manual. Issued in accordance with the National Industrial Security Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information. “Applies to all Executive Branch Departments and Agencies and all cleared contractor facilities located within the U.S. and its territories. It is to be used by contractors to safeguard classified information released during all phases of the contracting, licensing, and grant process, including bidding, negotiation, award, performance, and termination. It also applies to classified information not released under a contract, license, certificate or grant, and to foreign government information furnished to contractors that requires protection in the interest of national security.”

Document ID	Title & Location	Scope & Applicability
DOD 8581.1	Information Assurance (IA) Policy for Space Systems Used by the Department of Defense (8 June 2010) http://www.dtic.mil/whs/directives/corres/pdf/858101p.pdf	<p>Instruction. Implements requirements of NSD 42 by establishing IA policy and assigning responsibilities for all space systems used by the DOD in accordance with CNSSP-12. It provides the basic procedures for implementing IA for all DOD-owned, or controlled space systems used by the DOD regardless of MAC or CL.</p> <p>“Applies to OSD, the Military Departments, the office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the office of the Inspector general of the DOD, the Defense Agencies, the DOD Field Activities, and all other organizational entities in the DOD (collectively referred to as DOD Components). It applies to all DOD use of space systems and the components thereof (e.g., launch vehicles, satellites, payloads, launch and test ranges, satellite and network operations centers, and user equipment) to receive, process, store, display, or transmit classified or unclassified DOD information requiring controls. Including all DOD-owned, -controlled space systems, and all DOD use of commercial (domestic and foreign), and other USG, and, subject to the terms of international agreements, foreign government-owned space systems and the components thereof.”</p>
DOD 5200.1-M	Acquisition Systems Protection Program (March 1994)	<p>Guidance Manual. Prescribes standards, criteria, and methodology for the identification and protection of DOD Essential Program Information, Technologies, and/or Systems (EPITS) within DOD acquisition programs</p>
DODI 5200.39	Critical Program Information (CPI) Protection Within the Department of Defense	<p>Instruction. Establishes policy for the protection of CPI; Issues policy and assigns responsibility for counterintelligence (CI), Intelligence, Security, and Systems Engineering support for the identification and protection of CPI; Assigns responsibilities to DOD Components relating to the identification of CPI and the implementation of plans for its protection.</p>
DODI 5200.40	Information Technology Security Certification And Accreditation Process (DITSCAP) (30 December 1997) http://csrc.nist.gov/groups/SMA/fasp/documents/c&a/DLABSP/i520040p.pdf	<p>Rescinded by DODI 8510.01 (28 Nov 2007)</p>
DODI 8500.2	Information Security controls under DIACAP; Information Assurance (IA) Implementation (6 February 2003) http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf	<p>Instruction. Implements policy, assigns responsibilities, and prescribes for applying integrated, layered protection of DOD information system and networks. It established a baseline level of IA for all DOD information systems through the assignment of specific IA Controls to each system. Assignment is made according to MAC and CL.</p> <p>“Applies to the Office of the Secretary of defense, the Military Departments, the Chairman of the joint Chiefs of Staff, the Combatant Commands, the Inspector General of the DOD, the Defense Agencies, the DOD Field Activities, and other organizational entities in the DOD (referred to collectively as DOD Components).”</p>

Document ID	Title & Location	Scope & Applicability
DODI 8510.1-M	Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Manual (31 July 2000)	Cancelled by DODI 8510.01 (28 Nov 2007)
EO 12958	Executive Order 12958, (April 17, 1995), Classified National Security Information	Executive Order. Prescribes a uniform system for classifying, safeguarding, and declassifying national security information.
Report GAO-10-916	Information Security – Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems (September 2010) Government Accountability Office (GAO)	Report. “The objective of our review was to assess the progress of federal efforts to harmonize policies and guidance for national security systems and non-national security systems.”
NIST, 2009	Guide to NIST Information Security Documents http://csrc.nist.gov/publications/CSD_DocsGuide.pdf	Reference Guide to facilitate searching for particular NIST information security documents. “In addition to being listed by type and number, the guide presents the documents using three approaches to ease searching: by Topic Cluster, by Family, and by Legal Requirement.” Applies to all information security professionals with a need for NIST guidance, “especially those just entering the security field or with limited needs for the documents.”
ICD 503	Intelligence Community Directive Number 503: Intelligence Community Information Technology Systems Security, Risk Management, Certification and Accreditation (15 September 2008) http://www.odni.gov/electronic_reading_room/ICD_503.pdf	Directive. “Establishes Intelligence Community (IC) policy for information technology systems security risk management, certification and accreditation. It focuses on a more holistic and strategic process for the risk management of IT systems, and on processes and procedures designed to develop trust across the intelligence community IT enterprise through the use of common standards and reciprocally accepted C&A decision.” “Applies to the IC, as defined by the National Security Act of 1947, as amended, and other departments or agencies that may be designated by the President, or agency concerned, as an element of the IC.”
ICS 503-2	Intelligence Community Standard Number 503-2: Categorizing and Selecting Information Technology Systems Security Controls (Effective 21 May 2010)	Standard. Scope and applicability not available.

Document ID	Title & Location	Scope & Applicability
JCS Lexicon 2010	Joint Chiefs of Staff 2010 Cyber Operations Lexicon http://www.nsc.gov/CyberReferenceLib/2010-11-JointTerminologyforCyberspaceOperations.pdf	<p>Memorandum. Attachment establishes common lexicon for cyber operations.</p> <p>“... Though the language of Computer Network Operations, developed in the Information Operations context, has served us well, CO [Cyber Operations] has matured to the point where it should be aligned with other domains. ... For these reasons, I have tasked the Joint Staff to develop the attached lexicon to align CO vocabulary with standard joint terminology. This lexicon will be used as the starting point for normalizing terms in all cyber-related documents, instructions, CONOPS, and publications as they come up for review.”</p>
NIST SP 800-18 Rev. 1	Guide for Developing Security Plans for Information Systems (February 2006) http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf	<p>Guide. Provides basic information on how to prepare a system security plan (required by OMB Circular A-130, FISMA) and is designed to be adaptable in a variety of organizational structures and used as reference by those having assigned responsibility for activity related to security planning.</p> <p>“Applies to Program managers, system owners, and security personnel in the organization must understand the system security planning process. In addition, users of the information system and those responsible for defining system requirements should be familiar with the system security planning process. Those responsible for implementing and managing information systems must participate in addressing security controls to be applied to their systems.”</p>
NIST SP 800-30	Risk Management Guide for Information Technology Systems (July 2002).	<p>Superseded by draft version of SP 800-39 DRAFT Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View</p>
NIST SP 800-37 Rev. 1	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach (February 2010) http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf (A product of Joint Task Force Transformation Initiative)	<p>Guide. Satisfies the requirements of FISMA and provides guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. It ensures that managing information system-related security risks is consistent with the organization’s mission/business objectives and overall risk strategy established by the senior leadership; that information security requirements, including necessary security controls, are integrated into the organization’s enterprise architecture and system development lifecycle processes; supports consistent, well-informed, and ongoing security authorization decisions (through continuous monitoring), transparency of security and risk management-related information, and reciprocity; and aids achieving more secure information and information systems within the federal government through the implementation of appropriate risk mitigation strategies.</p> <p>Applies to “individuals associated with the design, development, implementation, operation, maintenance, and disposition of federal information systems including: Individuals with mission/business ownership responsibilities or fiduciary responsibilities; Individuals with information system development and integration responsibilities; Individuals with information system and/or security management/oversight responsibilities.”</p>

Document ID	Title & Location	Scope & Applicability
NIST SP 800-39	<p>"Managing Information Security Risk: Organization, Mission, and Information System View" (March 2011) http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf</p> <p>(A product of Joint Task Force Transformation Initiative)</p>	<p>Special Publication. "Provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems. It provides a structured, yet flexible approach for managing risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines. The guidance provided is not intended to replace or subsume other risk-related activities, programs, processes, or approaches that organizations have implemented or intend to implement addressing areas of risk management covered by other legislation, directives, policies, programmatic initiatives, or mission/business requirements. Rather, it is complementary to and should be used as part of a more comprehensive Enterprise Risk Management program.</p> <p>Applies to a diverse group of risk management professionals including: Individuals with oversight responsibilities for risk management; Individuals with responsibilities for conducting organizational missions/business functions; Individuals with responsibilities for acquiring information technology products, services, or information systems; Individuals with information security oversight, management, and operational responsibilities."</p>
NIST SP 800-53A Rev. 1	<p>Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, Revision 1 (June 2010) http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf</p> <p>(A product of the Joint Task Force Transformation Initiative)</p>	<p>Guide. Provides guidelines for building effective security assessment plans and a comprehensive set of procedures for assessing the effectiveness of security controls employed in information systems supporting the executive agencies of the federal government. It was developed to help achieve more secure information systems within the federal government by: Enabling more consistent, comparable, and repeatable assessments of security controls with reproducible results; Facilitating more cost-effective assessments of security controls contributing to the determination of overall control effectiveness; Promoting a better understanding of the risks to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems; and Creating more complete, reliable, and trustworthy information for organizational officials to support risk management decisions, reciprocity of assessment results, information sharing, and FISMA compliance.</p> <p>Applies to "a diverse group of information system and information security professionals including: Individuals with information system development and integration responsibilities; Individuals with information security assessment and continuous monitoring responsibilities; Individuals with information system and security management and oversight responsibilities; Individuals with information security implementation and operational responsibilities."</p>

Document ID	Title & Location	Scope & Applicability
NIST SP 800-53Rev. 3	<p>Recommended Security Controls for Federal Information Systems and Organizations (August 2009) http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf</p> <p>(A product of the Joint Task Force Transformation Initiative)</p>	<p>Special Publication. Provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, <i>Minimum Security Requirements for Federal Information and Information Systems</i>. The guidelines were developed to help achieve more secure information systems and effective risk management within the federal government by: Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems and organizations; Providing a recommendation for minimum security controls for information systems categorized in accordance with FIPS 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i>; Providing a stable, yet flexible catalog of security controls for information systems and organizations to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies; Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness; and Improving communication among organizations by providing a common lexicon that supports discussion of risk management concepts.</p> <p>Applies to “all components of federal information systems that process, store, or transmit federal information. It applies to: Individuals with information system or security management and oversight responsibilities; Individuals with information system development responsibilities; Individuals with information security implementation and operational responsibilities; and Individuals with information system and information security assessment and monitoring responsibilities.”</p>
NIST SP 800-59	<p>Guideline for Identifying an Information System as a National Security System (August 2003) http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf</p>	<p>Guide. Assists agencies in determining which, if any, of their systems are national security systems as defined by FISMA and are to be governed by applicable requirements for such systems, issued in accordance with law and as directed by the President.</p> <p>Applies to U.S. Government agencies requiring guidance in determining whether or not a system is classified as a National Security System (NSS).</p>

Document ID	Title & Location	Scope & Applicability
NIST SP 800-64Rev. 2	Security Considerations in the System Development Lifecycle http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf	<p>Special Publication. Provides “guideline is to assist agencies in building security into their IT development processes. This should result in more cost-effective, risk-appropriate security control identification, development, and testing. It focuses on the information security components of the SDLC (overall system implementation and development, and organizational information system governance process, is considered outside the scope of the document). First, it describes the key security roles and responsibilities that are needed in development of most information systems. Second, sufficient information about the SDLC is provided to allow a person who is unfamiliar with the SDLC process to understand the relationship between information security and the SDLC.”</p> <p>Applies to “a diverse federal audience of information system and information security professionals including: Individuals with information system and information security management and oversight responsibilities; Organizational officials having a vested interest in the accomplishment of organizational missions; Individuals with information system development responsibilities; and Individuals with information security implementation and operational responsibilities.”</p>
NSD-42	National Security Directive 42 – National Policy for the Security of National Security Telecommunications and Information Systems (5 July 1990) – Designates the Secretary of Defense and the Director of the National Security Agency as the Executive Agent and National Manager for national security systems, respectively. http://www.fas.org/irp/offdocs/nsd/nsd42.htm	<p>Directive. Establishes initial objectives of policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation. It is intended to ensure full participation and cooperation among the various existing centers of technical expertise throughout the Executive branch, and to promote a coherent and coordinated defense against the foreign intelligence threat to these systems. It recognizes the special requirements for protection of intelligence sources and methods.</p> <p>Applies to national security systems.</p>
NSPD-49	National Security Presidential Directive 49 – National Space Policy (31 August 2006) http://www.fas.org/irp/offdocs/nspd/space.html	<p>Policy. Establishes overarching national policy that governs the conduct of U.S. space activities.</p>

2.1.2 Technical Operating Reports from The Aerospace Corporation

Table 2-2. TORs

Document ID	Title	Scope & Applicability
TOR-2009(1455)-6	Advanced Cyber Threats to Satellite Communication Programs	Report. “This report is adapted from a white paper intended to provide recommendations for addressing information assurance issues relevant to the Transformational Satellite Communications System (TSAT) program. Analysis of the information assurance (IA) measures incorporated in that program identified some high-end cyber threats that had not been completely addressed and others that had not been addressed at all. In this report, actions that a program should take to ensure effective defense are identified, and illustrative comments relating to TSAT are provided.”
TOR-2010(8506)-7	Information Assurance: An Integral Component of Mission Assurance	Report. “This technical operation report (TOR) provides a high-level summary of the tasks performed by IA-SMEs in support of ensuring an adequate level of information assurance in a space system acquisition. It presents these tasks in a number of different views: by functional areas, by phase, and by core MA process areas. This TOR also includes a detailed mission assurance task list with respect to IA.”
TOR-2007(8583)-6702	Information Assurance Handbook for DOD Space Systems: Guidance on Application of DOD 8500.1/8500.2 IA Controls	Report. “[This report] analyzes and interprets each of the 8500.2 controls, providing an explanation and interpretation of the control and identifying issues with the Implementation Guidance and Validation Procedures. Every control is broken down by the area of responsibility of the major players in certification and accreditation for a large system acquisition: the program office, the developer/contractor, the operating command, and the certifier, with direction provided to program offices and operating command regarding their responsibilities and the evidence that they must produce. Each control is translated into language suitable for use in requirements documentation: a statement of work (developer process), an operational requirements document (system requirements), or data item descriptions (developer artifacts).”

2.2 Definitions

The following definitions provide a framework for common terminology as it applies to the topic of Space Segment Information Assurance. The definitions provided are often specific to this domain of discourse.

Term	Description ¹²
Accreditation	The “formal declaration by a Authorizing Official (AO) that an information system is authorized to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.” For the DOD, the AO is also referred to as the Designated Approval Authority (DAA).†
Authentication	A “security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.”
Authorizing Official (AO)	A government official with the ultimate responsibility of providing or withholding the system’s authority to operate (ATO). The AO is responsible to review certification artifacts and making a risk assessment prior to allowing, or disallowing system operations. By providing an ATO, the AO formally assumes responsibility for operating a system, asserting that such operation will be at an acceptable level of risk. The AO is generically responsible for the adequacy of security controls. [In DOD, the Designated Approval Authority (DAA)]
Availability	“Timely, reliable access to data and information services for authorized users.” Note: This usage differs from the typical engineering view of “availability”, which is expressed in terms of Mean Time Between Failure (MTBF) and Mean Time to Repair (MTTR). “Availability”, in the IA sense, captures the notion that information and systems are accessible and usable when they are needed even during cyber attacks. †
Certification	The “comprehensive evaluation of the technical and nontechnical security safeguards of an IS [information system] to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.”
Compromise	The “disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.”
Confidentiality	“Assurance that information is not disclosed to unauthorized individuals, processes, or devices.”
Confidentiality Level ¹³ (CL)	Determination/identification of whether the system processes classified, sensitive, or public information.
Cyberspace ¹⁵	Domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.

¹² Definitions in quotes are based upon those in CNSSI No. 4009, Information Assurance (IA) Glossary, revised April 2010. Some CNSSI 4009 definitions are expanded slightly; this is indicated with †. Definitions and terms marked with footnotes are from alternate sources. Definitions with no special markings of any kind are defined by the author / contributors to this document for the purpose of use herein.

¹³ Other unidentified sources.

Term	Description ¹²
Cyber ¹⁴	Informally and widely used as a prefix modifier used to describe, for example, processes conducted in, through, or about aspects of Cyberspace, conditions of elements of Cyberspace, etc. However, also often used in more specific ways for specific purposes. For example, Cyber Security, Cyber Warfare, and Cyber Mission Assurance as defined and used herein.
Cyber Mission Assurance ¹⁴	The disciplined application of proven scientific, engineering, quality and program management principles toward the goal of achieving mission success with or regarding systems established in whole or part in Cyberspace. [Also see Mission Assurance]
Cyber Security ¹⁵	All organizational actions required to ensure freedom from danger and risk to the security of information in all its forms (electronic, physical), and the security of the systems and networks where information is stored, accessed, processed, and transmitted, including precautions taken to guard against crime, attack, sabotage, espionage, accidents, and failures. Cyber Security risks may include those that damage stakeholder trust and confidence, affect customer retention and growth, violate customer and partner identity and privacy protections, disrupt the ability to conduct or fulfill business transactions, adversely affect health and cause loss of life, and adversely affect the operations of national critical infrastructures.
Cyber Warfare ¹⁵	An armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defense, and cyber enabling actions.
Evaluation Assurance Levels (EAL 1-7) ¹⁶	EAL1 – functionally tested EAL2 – structurally tested EAL3 – methodically tested and checked EAL4 – methodically designed, tested and reviewed EAL5 – semi-formally designed and tested EAL6 – semi-formally verified design and tested EAL7 – formally verified design and tested
IA control ¹⁷	“An objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text, and a control class). Specific management, personnel, operational, and technical controls are applied to each DOD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with OMB Circular A-130.” A system’s <i>requisite IA controls</i> are those IA controls required by DOD or government policy – that is, those that would be called out by the baseline appropriate for the categorization of the system – that have then been tailored based on the system’s threat environment, and subsequently incorporated into the system’s statement of requirements.

¹⁴ Defined for use herein only.

¹⁵ Joint Chiefs of Staff, “Lexicon for Cyber Operations”, 2010.

¹⁶ Common Criteria User Guide, October 1999, page 8.

¹⁷ DoDD 8500.02, “Information Assurance (IA) Implementation,” 6 February 2003, page 20.

Term	Description ¹²
Information Assurance	Those “measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.” Information Assurance ensures that accurate information is shared with those authorized to access it, and is available when it is needed. †
Integrity	The “quality of an IS reflecting the logical correctness and reliability of the operating system and other underlying mechanisms; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security model, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.” Integrity helps to ensure that information provided to an end user has not been maliciously altered. †
Mission Assurance Category I (MAC I) ¹³	Information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.
Mission Assurance Category II (MAC II) ¹³	Information that is important to the support of deployed and contingency forces.
Mission Assurance Category III (MAC III) ¹³	Information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term.
Mission Assurance ¹⁸	The disciplined application of proven scientific, engineering, quality and program management principles toward the goal of achieving mission success.
National Security Systems (NSS) ¹³	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency-- (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Non-repudiation	“Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.”
Risk Management Framework (RMF) ¹³	Structured process that integrates information security and risk management activities into all phases of the system development lifecycle.
UCDMO ¹	Unified Cross Domain Management Office – All DOD and IC cross domain efforts are under jurisdiction of this office. (Established July 2006) http://www.ucdmo.gov

¹⁸ From the Memorandum of Understanding among Air Force Space and Missiles Systems Center, National Reconnaissance Office, Missile Defense Agency, and National Aeronautics and Space Administration, 2 February 2011.

Term	Description¹²
Vulnerability	A “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.”

2.3 Acronym List

Acronym	Description
AO	Authorizing Official (e.g., in DOD, the DAA)
ASIC	Application Specific Integrated Circuit
ATO	Authority to Operate
C&A	Certification and Accreditation
C,I,A	Confidentiality, Integrity, and Availability
CA	Certification Authority
CDRUSSTRATCOM	Commander, United States Strategic Command
CDR	Critical Design Review
CDS	Cross-domain Solution
CL	Confidentiality Level
CMA	Cyber Mission Assurance
CMMA	Cyber Management and Mission Assurance
CMMI	Capability Maturity Model Integration
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COA	Course of Action
COMSEC	Communications Security
COTS	Commercial off the Shelf
Cyber SA, CSA	Cyber Situational Awareness
DAA	Designated Approval Authority
DCID	Director of Central Intelligence Directive
DIACAP	DOD Information Assurance Certification and Accreditation Process
DISA	U.S. Department of Defense Information Systems Agency
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DNI	Director of National Intelligence
DOD	Department of Defense
DODI	Department of Defense Instruction
DoS	Denial of Service
EAL	Evaluation Assurance Level (Common Criteria defined level of assurance)
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standard (Mandatory Standard)
FISMA	Federal Information Security Management Act, December 2002

Acronym	Description
FPGA	Field Programmable Gate Array
FW	Firmware
GAO	Government Accountability Office
HDL	Hardware Description Language
HR	High Robustness
HW	Hardware
IA	Information Assurance
IARMP	Information Assurance Risk Management Program
IASRD	Information Assurance Security Requirements Document (NSA Type 1 requirements)
IC	Intelligence Community
ICD	Intelligence Community Directive
IP	Intellectual Property
IS	Information System
ISSE	Information System Security Engineering
IT	Information Technology
JAFAN	Joint Air Force - Army - Navy
JHU/APL	Johns Hopkins University Applied Physics Lab
JTF-GNO	Joint Task Force for Global Network Operations
JTFTI	Joint Task Force Transformation Initiative
MA	Mission Assurance
MAIW	Mission Assurance Improvement Workshop
MAC	Mission Assurance Category
MAG	Mission Assurance Guide
MDD	Material Development Decision
MIDM	Mission Information Dependency Maps
MS	Milestone
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NIACAP	National Information Assurance Certification and Accreditation Process (April 2000) http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NISCAP	NSA/CSS Information Systems (IS) Certification and Accreditation Process
NISPOM	National Industrial Security Program Operating Manual (DOD 5220.22-M) (28 February 2006) http://www.dss.mil/isp/odaa/documents/nispom2006-5220.pdf
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NSC	National Security Community

Acronym	Description
NSD	National Security Directive
NSI	National Security Information as defined in Executive Order 12958
NSPD	National Security Presidential Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSS	National Security Systems
NSS-S NSS-Space	National Security Systems – Space. Also used in this Guide to designate “National Security Space” which is shorthand for National Security Systems – Space.
OBJ	Objective
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OS	Operating System
OSD	Office of the Secretary of Defense
PDR	Preliminary Design Review
PPP	Program Protection Plan
PUB	Publication
RMF	Risk Management Framework
SABI	Secret and Below Interoperability
SC	Security Categorization
SCI	Sensitive Compartmented Information
SCRMP	Supply Chain Risk Management Plan
SDR	System Design Review
SDLC	System Development Lifecycle
SE&I	System Engineering and Integration
SETA	System Engineering and Technical Assistance
SIPRNET	Secret Internet Protocol Router Network
SKPP	Security Kernel Protection Profile
SLOC	Source Lines of Code
SOC	Satellite Operations Center
SP	Special Publication (NIST Special Publications)
SS	Space Segment
SSMP	System Security Management Plan
STAR	System Threat Assessment Report
STIG	Security Technical Information Guide
SW	Software
TBD	To Be Determined
TCNO	Time Compliance Network Order
TOR	Technical Operating Report
TRANSEC	Transmissions Security

Acronym	Description
TSABI	Top Secret/SCI and Below Interoperability
TT&C	Telemetry, Tracking, and Command
TTPs	Tactics, Techniques and Procedures
UARC	University Affiliated Research Center
UCDMO	Unified Cross Domain Management Office
U.S.	United States
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USG	United States Government

3. Applicable Governance, Standards, Guidance

NSS-S system developers and operators must prevail against daunting challenges to protect against mission disruption, service denial, performance degradation, and mission destruction or loss in the face of emerging and constantly changing security threats, and revolutionary changes in the use and mission of spacecraft. As the number of threats increases, there is a corresponding increase in the numbers of entities capable of exercising threats and exploiting system vulnerabilities resulting in increased mission risk for NSS-S developers, operators, and mission end-users and consumers. Combating these challenges requires a common risk-based information assurance approach (chapter 3) along with adaptable, mission-specific security controls and techniques to ensure uninterrupted mission operations continuity (chapter 4).

Chapter 3 discusses recognized mandatory standards, governance, and guidance that must be considered when developing new or supporting operational or legacy space systems. This chapter provides (1) a brief historical overview of IA practices within the federal government and associated difficulties and challenges, (2) current IA practices with respect to the space segment, and (3) convergent and transformative activities that are currently taking place to establish ubiquitous IA standards across the federal government.

[**Note to the reader:** This chapter cites numerous governance, standards, and guidance that were known to be accurate at the time of this writing (March 1, 2011). Due to the highly dynamic nature of the material addressed in chapter 3, please refer to authoritative sources after this time to ensure that the most current data is referenced with respect to this TOR.]

3.1 Context: Past, Present, and Future

In December 2002, the Federal Information Security Management Act (FISMA)¹⁹ was passed to provide a comprehensive framework that ensures the effectiveness of information security controls over any information resources that support federal operations and assets. FISMA, and other authoritative agency governance, drives ALL federal agencies to develop standards and processes to facilitate:

- Periodic assessments of risk
- Risk-based policies and procedures
- Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate
- Security awareness training for agency personnel, including contractors and other users of information systems
- Periodic testing and evaluation of information security procedures and practices, performed with a frequency depending on risk, but no less than annually
- A process for planning, completing, evaluating and documenting remedial action to address deficiencies
- Procedures to detect, report and respond to security incidents
- Plans and procedures to ensure continuity of operations

The National Institute of Standards and Technology (NIST) FISMA Implementation Team developed the Risk Management Framework being utilized by Civil Federal agencies. Now, the Joint Task Force Transformation Initiative (JTFTI) Working Group comprised of key representatives from the NIST, Department of Defense, Office of the Director of National Intelligence, and the Committee on National

¹⁹ H.R. 2458 E-Government Act, Public Law 107-347, Title III

Security Systems (CNSS) are working together to implement a unified, risk-based, information security framework for the federal government.

3.1.1 Past

Securing systems has long been a concern for federal agencies. Many policies and directives have been issued over the years that require agency officials to protect and secure information systems, data transmission, and data including *National Security Directive 42*²⁰ and *National Security Presidential Directive 49*²¹ to name two. The DOD and IC have played a pivotal, leading role in establishing and promulgating governance and implementation guidance to protect our nation’s space assets, supporting information systems and data, providing every advantage possible for our war fighters.

Until very recently, the IC, DOD, ODNI, and Civil Federal agencies have had area- or agency-specific Information Assurance guidance as shown in Table 3-1 below:

Table 3-1. Area- and Agency-Specific IA Guidance Examples

IA Guidance		Agency
DCID 6/3	Protecting Sensitive Compartmented Information Within Information Systems – Manual, Updated April 20, 2004	Director of Central Intelligence (IC Systems)
DODI 5200.40	DOD Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997	Department of Defense (DOD Systems)
DODI 8510.01	DOD Information Assurance Certification and Accreditation Process, November 28, 2007	
DOD 5220.22-M	National Industrial Security Program Operating Manual, February 28, 2006	
JAFAN 6/3	Protecting Special Access Program Information Within Information Systems, October 15, 2004	
NSTISSI No. 1000	National Information Assurance Certification and Accreditation Process (NIACAP), April 2000	Committee on National Security Systems (National Security Systems)
NISCAP	National Security Agency/Central Security Service Information Security Certification and Accreditation Process	National Security Agency / Central Security Service
NIST SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004 (Note: Revision 1 update in February 2010)	National Institute of Standards and Technology (Civil Federal Systems)
NIST SP 800-53 Rev 1	Recommended Security Controls for Federal Information Systems, December 2006 (Note: Revision 3 update in August 2009)	

Although the DOD, IC, and Civil Federal government agencies diligently developed and implemented *similar* measures to protect government systems and assets, the *differences* in agency-specific guidance have caused unintentional and costly problems that have most notably manifested themselves when

²⁰ National Policy for the Security of National Security Telecommunications and Information Systems (5 July 1990)

²¹ National Space Policy (14 September 1996)

agencies have worked together on joint programs and projects. Many of the problems encountered due to agency-specific IA approaches are briefly discussed below.

3.1.1.1 Reciprocity

While each agency developed their own approach to securing government assets, the processes, key terms, review, testing, and accrediting processes differed across DOD, IC, and Civil Federal areas resulting in severely limited recognition of “established” security posture across area boundaries. This has resulted in very costly security reviews, late-in-the-SDLC requirements changes (increased costs), and numerous program and project delays while area AOs agree/disagree on the trustworthiness and security preparedness of systems.

3.1.1.2 Trust

As discussed in the previous section, key system(s) components (command and control, data transmission, customers/consumers, and others) residing in DOD, IC, or Civilian Federal space have been problematic due to the unforeseen barriers caused by the disparate governance in each area. Re-tests, reviews, reaccreditation, requirement changes, and delays have often resulted due to lack of knowledge, familiarity, and comfort with one agency’s IA approach versus another agency’s approach.

3.1.1.3 Disparate Controls (Area-Specific Governance and Policies)

Related to trust and reciprocity, each area has produced and implemented a catalog of security control requirements that are used to protect government systems and assets. Because agencies from each area took a separate approach in naming, quantifying, and testing security controls – the same or very similar security controls may not be recognizable “as the same” as implemented in another area’s agency guidance. This, again, has resulted in re-tests, reviews, reaccreditation, requirements changes, delays, and increased costs to design, develop, implement, and operate program and mission assets.

3.1.1.4 Lack of Mutual Terminology/Lexicon

One of the root causes of the problems illustrated above is the existence and use of different terminology across areas. Many key terms have been defined locally – at the agency level, versus globally – at the federal level, resulting in confusion, cost increases, delays, and re-work.

3.1.1.5 Risk Management at System Level

Another by-product of the disparate IA approaches has been differences in risk management. Several agencies have taken a system-level perspective at managing risk, while others have taken an overall mission view. The drastically different perspective in risk level interpretation has made agencies uncomfortable with cross-agency certification and accreditation results and contributed to lack of reciprocity (discussed earlier). Identifying sub-system reliance, key system interconnections, and other foundational dependency considerations late in the SDLC have caused additional cost increases, delays, and re-work.

3.1.1.6 IA Micro/Macro System View

Similar to the discussion in the Risk Management section, micro and macro perspectives on security control scoping, inheritance, and common controls have been another source of problems related to disparate IA approaches across areas. Increased costs and delays due to security control duplication and

non-reliance on available, common controls meant for specific purposes, are all systemic problems related to a heads-down, micro view of a system – versus an enterprise or mission view.

3.1.1.7 System Development

Sound, disciplined system engineering and development practices across government areas have been optimized and refined over time but are reflective of the area- or agency-specific IA guidance. Security control requirements and related development requirements have not been consistently included in system requirements baselines resulting in cost increases, delays, and other related problems.

3.1.2 Present – Harmonization and Transformation in Progress

Currently, United States Government space segment assets are subject to DOD, CNSS, and/or IC IA governance standards dependent upon the use of the system and the type of data processed. The foundational governance standards in use are listed in the Table 3-2 below:

Table 3-2. Foundational Governance Policies and Standards

Standard/Policy	Agency
DODI (Department of Defense Instruction) 8581.1, <i>Information Assurance (IA) Policy for Space Systems Used by the Department of Defense</i> (Revised 8 June 2010)	Department of Defense (DOD)
ICD-503 (Intelligence Community Directive) for <i>Intelligence Community Information Technology Systems Security, Risk Management, and Certification and Accreditation</i> (September 2008)	Office of the Director of National Intelligence (ODNI)
CNSSP 12 <i>National Information Assurance Policy for Space Systems Used to Support National Security Missions</i> (March 2007)	Committee on National Security Systems (CNSS)
CNSSP 6 <i>National Policy on Certification and Accreditation of National Security Systems</i> (2005)	
CNSSI-1253 (Committee on National Security Systems Instruction) <i>Security Categorization and Control Selection for National Security Systems</i> (October 2009)	
CNSSP-22 <i>Information Assurance Risk Management Policy for National Security Systems</i> (February 2009)	

The main selection criterion for governance applicability in the space segment is determined by the type of data processed by the system. Table 3-3 shows applicable guidance based on data processed by the space system. If the space system processes DOD collateral (Top Secret and below) information then DOD 8581.01 applies. For space systems designated as a National Security System (NSS) or processes National Security Information (NSI) then CNSSP 12 applies. For space systems that process SCI data then ICD-503 applies. CNSSP 12 applies to all DOD and IC space systems and DOD 8581.01 is the DOD implementation of CNSSP 12.

Key representatives from NIST, DOD, ODNI, and CNSS are working together in the Joint Task Force Transformation Initiative (JTFTI) Working Group to implement a unified, risk-based, information security framework for the entire federal government. In the near future, the DOD, IC, and Civil Federal agencies

will follow a common risk management framework based on NIST SP 800-30, -37, and -39 and a common security control catalogue based upon NIST SP 800-53 Revision 3 (note: CNSSI 1253 establishes which controls from NIST SP 800-53 apply to NSS).

Table 3-1. Governance Selection/Applicability Criteria

Type of Data	Applicable Guidance
DOD Collateral Information (Top Secret and Below)	DOD 8581.01 CNSSP-12
National Security Information (Classified or Unclassified)	CNSSP-12
SCI Intelligence Data	ICD-503 CNSSP-12

3.1.2.1 DODI 8581.1/8500.2

DOD 8581.01 governs space systems IA protection for all DOD sponsored, owned, operated, and leased space assets that process DOD collateral level (or lower) data.

The DOD information security policy, documented in DOD Instructions 8500.01²² (DIACAP) and 8500.2²³ (security controls), drives the DOD IA process illustrated in Figure 3-1. Many of the recognized roles and responsibilities outlined in DOD’s approach are very similar to those contained within the risk management framework methodology outlined in NIST SP 800-37, CNSSP 22, and CNSSI 1253.

Per the Government Accountability Office (GAO) Report GAO-10-916²⁴– (paraphrasing) DOD plans to transition to the unified risk management framework and common control catalog by first revising the 8500 series of guidance. Revisions to directive 8500.01(IA defense-in-depth), instruction 8510.01 (DIACAP), and instruction 8500.2 (security controls) based on the risk management framework described in CNSS Policy 22, and the security control catalog found in CNSSI-1253 and NIST SP 800-53 (revision 3) are expected as soon as December 2011. A schedule for additional implementation and assessment guidance, technical instructions, and other information that follow the major policy and instruction revisions is expected in 2011.

²² DoD Information Assurance Certification and Accreditation Process (DIACAP)

²³ Information Assurance (IA) Implementation

²⁴ Information Security – Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems (September 2010)

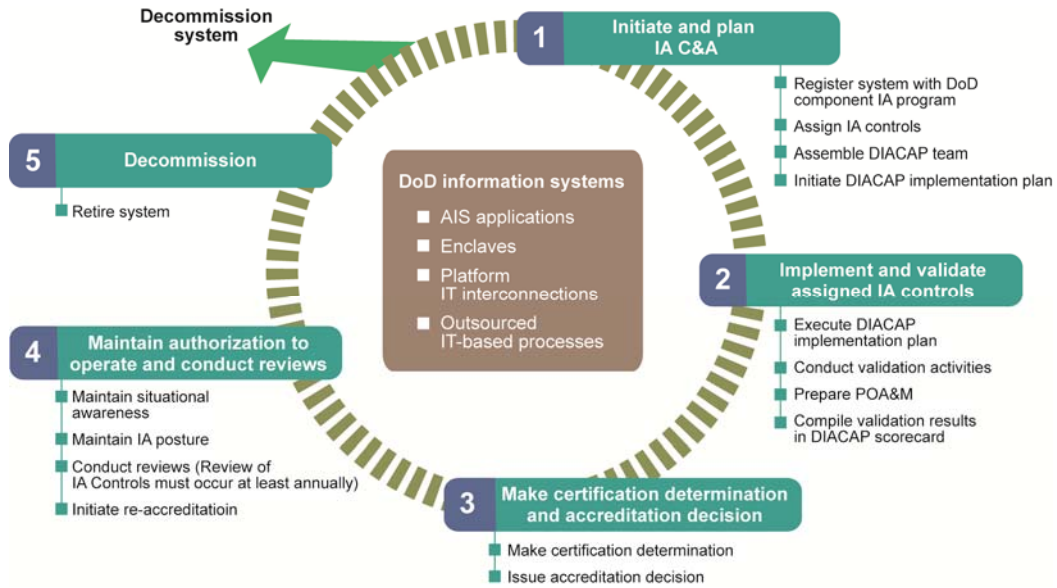


Figure 3-1. DIACAP²² security lifecycle.

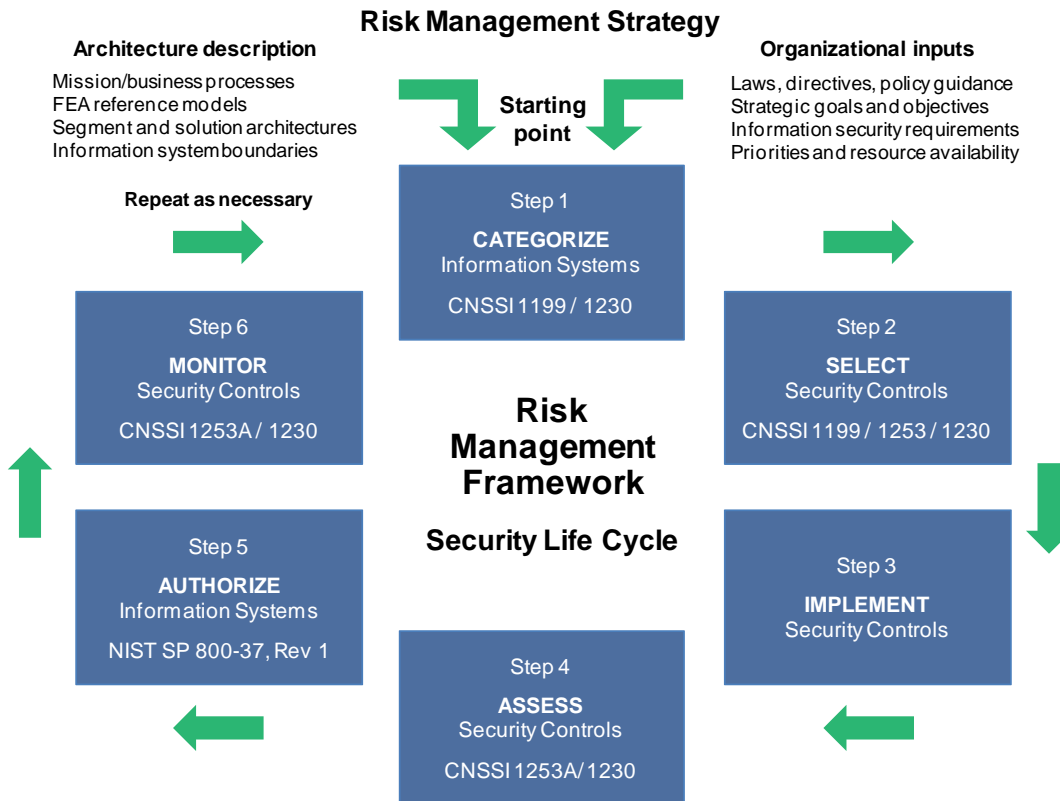


Figure 3-2. Risk management framework security lifecycle.

3.1.2.2 ICD-503/CNSSP 22

Figure 3-2 contains the Risk Management Framework as mandated by the ICD-503 and documented in the CNSSP 22 document. CNSSP 22 incorporates the use of CNSSI 1253 containing the NIST SP 800-53 security control catalog. The Risk Management Framework has been previously adopted by Civil Federal Agencies and is currently being adopted by the DOD and the IC communities. The framework is very similar to current processes being followed by DOD agencies and a mapping of DIACAP to the Risk Management Framework is provided for comparison in Figure 3-3.

3.1.2.3 JTFTI Unified Information Security Framework

The Joint Task Force Transformation Initiative (JTFTI) Working Group was established in April 2009 and is comprised of membership from the CNSS, ODNI, DOD, and NIST. The JTFTI's primary goal is to establish a unified information security framework for the federal government that leverages leading practices from the DOD, intelligence community, and civilian agencies. Converged and harmonized security governance will result in more effective security control implementation across interconnected systems, reduced duplication of effort and markedly reduced maintenance costs while making it more simple for vendors and contractors to provide IA-related products and services to the federal government.

Additional JTFTI Working Group Goals:

- Establish Reciprocity
- Achieve Common Trust Levels
- Adopt Common Body of Security Controls
- Adopt Common Terminology
- Risk Management at Enterprise Level
- IA Delivery as Enterprise Service
- Development life-cycle inclusive of IA

Five foundational NIST documents aligned with ODNI, DOD, IC, and CNSS contain harmonized information security guidance. Four of the five have been completed and one remains under development as shown in Table 3-4.

Table 3-4. Publication Status of Foundational NIST Harmonization Documents

Guidance/Publication	Issue Date/Status
NIST SP 800-53, revision 3, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>	Released August 2009
NIST SP 800-37, revision 1, <i>Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach</i>	Released February 2010
NIST SP 800-53A, revision 1, <i>Guide for Assessing the Security Controls in Federal Information Systems and Organizations</i>	Released June 2010
NIST SP 800-39, <i>Enterprise-Wide Risk Management: Organization, Mission, and Information Systems View</i>	Released March 1, 2011
NIST SP 800-30, revision 1, <i>Guide for Conducting Risk Assessments</i>	Spring 2011 (anticipated release)

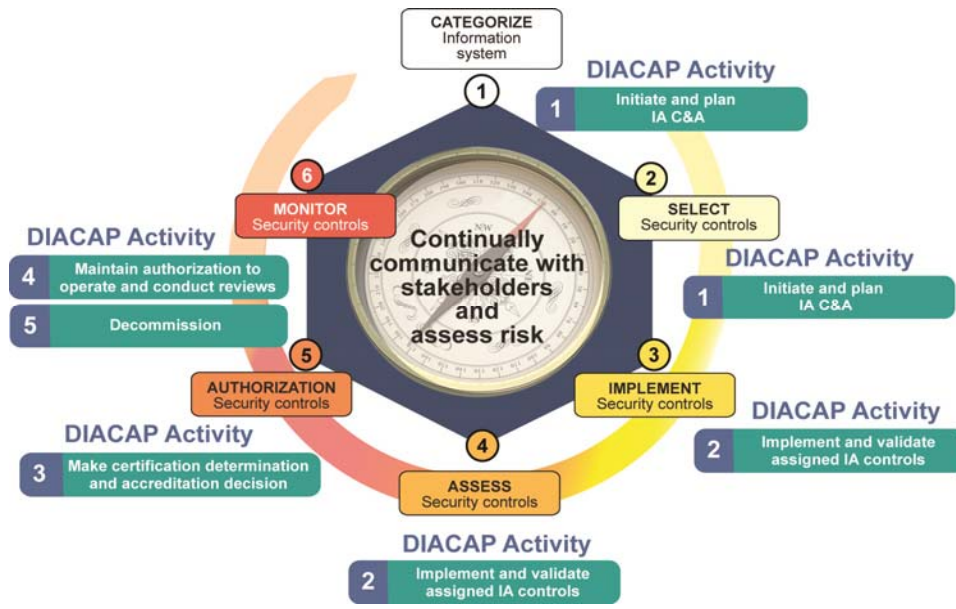


Figure 3-3. Alignment of DIACAP with risk management framework.

Additionally, CNSS will issue a revision (anticipated December 2011) of National Security Systems Policy No. 6²⁵ that will direct the use of NIST SP 800-37 and SP 800-53A. Figure 3-4 illustrates the key areas that have been targeted for harmonization, including: risk management approach, security categorization (basis to establish IA protection needs), security controls (security requirements and safeguards that will protect a system), security assessment procedures (methodology to test security controls to see if they are adequate and are working as intended), and security authorization (certification and accreditation).

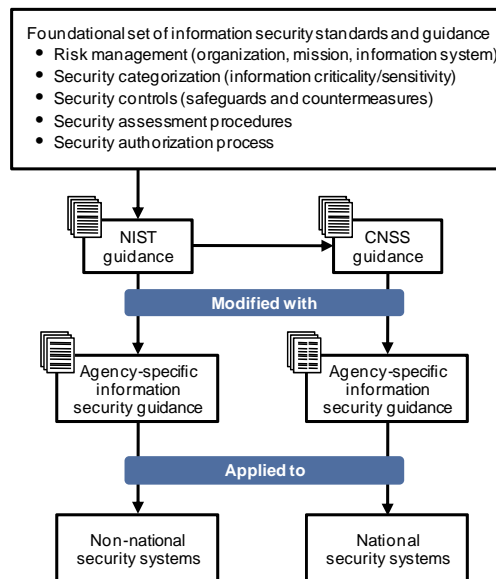


Figure 3-4. Areas targeted for harmonization.

²⁵National Policy on Certification and Accreditation of National Security Systems

The main differences in the current DOD processes and those under the JTFTI Unified Risk Management Framework are the use of a common security control catalog, a common Certification and Accreditation approach, and a mission versus system-based impact approach. For a description of the steps comprising the Risk Management Framework, see Appendix A.

<p>Guideline 3-1. Be Cognizant of NSS IA Guidance Changes</p> <p>Recommendation: The JTFTI including CNSS, ODNI, DOD, and NIST are revising and promulgating policy and guidance that aligns with the NIST SP 800-53 security control catalog, SP 800-53A security control assessment guide, and SP 800-37 risk management guide. Programs, especially those in early phases of the SDLC, should keep a close eye on changes and related impacts to program requirements baselines, costs, and schedules.</p>
<p>Evaluation Criteria: Program understands exactly what impending changes could impact program requirements, baselines, costs, and schedules.</p>
<p>Milestone: MDD/A/B</p>
<p>Rationale: All federal government agencies are moving toward a common risk management framework based on the use of a government-wide security control catalog.</p>
<p>Stakeholders/Actions: Program Office: Using program office personnel (including FFRDCs) or using development contractors, define and fund tasking to track and evaluate for impact planned changes in IA policy standards and guidance as they apply to program.</p>

3.1.3 Future Expectations

3.1.3.1 Legacy / Operational Systems

Recognizing the limited ability to enact change on legacy and operational space systems, the governance change impact on system owners, managers, and operators poses new challenges. Legacy-systems support organizations should be prepared to undertake activities like assessing and reporting significant gaps between deployed controls and those in the new control catalog. They should also be prepared to assess and report on mission impact of proposed changes to the legacy/operational system baselines, and to revise continuous monitoring plans accordingly. Again, because of the limited ability to make changes in this environment, there are no plans to require wholesale security control retrofits for deployed systems.

3.1.3.2 Developing Systems

Programs that are in early requirements phases of the SDLC should pay close attention to the changing governance within the DOD and IC realms. In many cases, developing IC programs are already required to adhere to the new governance unless specifically directed differently by agency officials. The DOD is currently revising or planning to revise many of its governance pillars to align with the unified risk management framework, including the SP 800-53 control catalog. Program officials should carefully monitor governance revision schedules for changes that potentially impact program costs and schedules.

3.2 Common Governance and Risk Management Framework Are Not Enough

Establishing common governance using a risk-based, managed approach across agency boundaries is an important first step in further securing vital national space assets. The resultant common lexicon, security controls, IA SDLC, and certification and accreditation perspective are anticipated to sharply reduce many

of the issues that have been discussed in this section. The following sections of this document provide guidelines focusing on best practices that will help secure space assets.

The discussion in chapter 3 assumes that space segment systems and programs have met the intent of the required security controls for their system, which is by no means assured. Chapters 5, 6, and 7 include guidance designed to go above “checking the boxes” toward meeting the intent.

Unfortunately, that is not enough to guarantee the space asset is secure. What happens when a would-be Cyber attacker metaphorically drives around the gate, swims across the moat, or tunnels under the perimeter? Chapter 4 meets this question head-on with an analysis of how to think about this challenge and how to meet it (with appropriate general guidance), and chapters 5, 6, and 7 also include guidance designed to implement the general guidance found in chapter 4.

4. Establishing a Cyber Mission Assurance Framework

Chapter 3 documented the existing baseline of governance, standards, and guidance available for application to Space Systems. While these are critical and necessary, even when done well, they are *insufficient* to achieve mission assurance in the current and future cyber environment. This chapter proposes an extensible framework for assessing, managing, and addressing cyber dependencies, risks, and threats. It is intended to provide a context for current day activities as well as an informed roadmap for emerging programmatic, development, and operational decisions.

This chapter envisions a more robust and capable set of cyber mission assurance capabilities than currently exists, although mechanisms and initiatives exist to allow progress. Chapter 4 should be used to *understand the full scope of the desired mission assurance capabilities* and to *guide policy and process changes*. While these evolve, however, programs still need actionable guidance that is achievable today. Chapters 5, 6, and 7 are directly traceable to chapter 4 and provide those actionable guidelines. It is expected that the community-wide policies and mechanisms *will* continue to evolve towards enabling the goals in chapter 4. As a result, the corresponding actions and guidelines in chapters 5, 6, and 7 will also evolve.

Information Assurance and the more expansive realm of *cyber operations* is a rapidly evolving field in every aspect: technologies, policies, threats, and operational acceptance. Recommendations made regarding IA and Cyber Mission Assurance for Space Segments of Space Systems must be made within the context of this dynamic environment. However, it should be understood that – at its core – the mission assurance goals and strategies for Space Systems do not dramatically change when considering cyber and IA. We still seek to prioritize mission-critical components and operations, maintain continuity of operations, and understand critical program information. But the nature of the cyber environment introduces three aspects perhaps not previously recognized for Space Systems:

1. Global Reach: When operating via cyber means, our adversaries do not require physical access to our facilities. Thus the scope of risk is dramatically expanded and our mission assurance approach must accommodate that.
2. At-Network Speed: Cyber-based mission risks, intentional or unintentional, benign or malicious, will occur at network speeds, often simultaneously. Recognition, response, and restoration of mission capability must be enabled at network speeds. Traditional risk mitigation approaches and continuity of operations plans cannot accommodate this.
3. Pace of Threat/Risk Evolution: Unlike other threat sources, cyber-based threats cannot be tightly tied to a particular source – today’s cutting edge approach, available only to the most sophisticated entities, will easily be available for purchase and reuse in short periods of time, and the ‘cutting edge’ will continually be redefined. Our approach to mission assurance must be sufficiently flexible and enduring to adapt to this reality.

Overall, as shown in Figure 4-1, a cyber-ready mission assurance approach starts with familiar questions:

- Who/What Can Affect Me? - What is the scope of connection to our systems? When considering cyber-based connections, that scope extends to inter-connected networks, contractor development facilities and corporate networks, test equipment and scripts, etc.
- How Will I Know What Is Happening? – If cyber-based problems occur, how would those be recognized, managed, and mitigated? How will we instrument, measure, and determine mission readiness of our systems?
- What Is The Impact On Mission? – Do we understand the dependencies between our cyber infrastructure, our mission information, and our critical mission operations? Which risk areas

should receive priority and allocation of resources? What are the potential effects on my mission globally if I take localized action on my network?



Figure 4-1. Preparing for a cyber-ready mission assurance framework.

These questions guide the flow of the rest of chapter 4. Section 4.1 addresses Cyber Mission Assurance *Enablers*, the capabilities and initiatives that must exist to segment, extend, or modify the existing Governance and Standards. Section 4.2 describes the Cyber Mission Assurance *Application Areas* across which these initiatives must span, emphasizing that this is a life-cycle-long process. Section 4.3 identifies the Cyber Mission Assurance *Participants*, those stakeholders and entities who hold direct responsibility for achieving these capabilities. Section 4.4 provides a mapping between the enablers (4.1) and the application areas (4.2), describing the activities across the lifecycle and identifying the key outcomes that are needed. From this mapping, we derived the guidelines captured in section 4.5 and identified the specific roles of the affected participants (4.3) in achieving them.

This is intended to set the stage for cyber mission assurance activities. Top level guidance is provided for the establishment of the approach, and then the application of those findings impact each of the following sections provided in this document.

4.1 Information Assurance/Cyber Security *Enablers* for Mission Assurance

Since the publication of the Trusted Computer System Evaluation Criteria (TCSEC) in the mid 1980s, IA emphasis in defense and national security systems has been largely vulnerability-based, equating the patching of known vulnerabilities with a reduction in IA risk. As a result, technologies and policies have evolved first and foremost to address the governance of system configuration and policy. While this configuration emphasis allows for a consistent baseline, it artificially provides the impression that compliance with security configuration policy equates to reduced risk. Mission assurance in a cyber context requires that our cyber security policies and solutions extend past configuration compliance and governance. We must transition from an environment of *risk avoidance* – defined and measured by the number of vulnerabilities identified and the state of patches to address them – to an approach of *risk management*. Thus, IA/CS decisions – both in development and operations – should be informed by how dependent the mission is on the information being protected and whether mission operations can successfully complete, regardless of the state of cyber configuration or the actions of adversaries operating against those systems.

To establish that cyber-ready mission assurance approach, there are three key enablers that must exist beyond existing governance. They are shown in Figure 4-2. These enablers involve activities, analyses, or products during every phase of the system lifecycle.

As stated earlier, governance, and compliance with it and existing standards are *also* key enablers for cyber mission assurance. However, for the purposes of this section, we look in more detail at the extensions. These are:

1. Mission-Driven Assessment
2. Access Understanding/Control
3. Instrumentation/Measurement/Trust

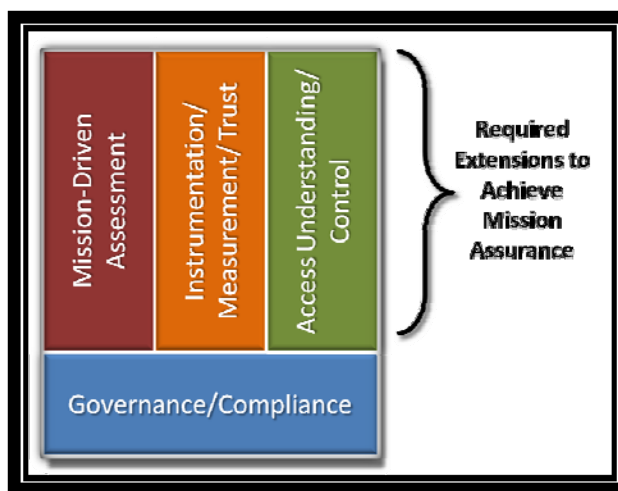


Figure 4-2. Extending existing approaches to handle dynamic cyber environment.

While listed sequentially, each is tightly inter-related to the others. For each of these, we seek to establish a consistent method and approach for assessing that area, capturing key dependencies, and accommodating for the maturation of our system, operations, and threat understanding. Each of the key constituencies in the design, development, and operations of Space Systems must make the commitment of resources to establish and maintain these functions throughout the system lifecycle.

4.1.1 Mission-Driven Assessment

The first cyber mission assurance enabler we discuss is the need for performing, maintaining, and exercising a Mission-Driven Assessment of the Space Systems. The term Mission-Driven Assessment here refers generically to a combined set of processes that determine and capture the relationship between a Space System cyber environment, the mission critical information that we try to assure, and the mission outcome itself. A limited version of these ideas are expressed in existing governance mandates to conduct program protection planning, and later chapters of this guidance document will pick up on that relationship²⁶.

Mission-Driven Assessment involves analyzing and capturing the mission-to-information dependencies sufficiently to derive risk to mission given a current cyber state and to use those dependencies to drive

²⁶ The specific process components and examples discussed here, however, originate with the Johns Hopkins University Applied Physics Laboratory (JHU/APL) Cyber Measurements and Mission Assurance (CMMA) models and processes. For further information on CMMA, contact Wende Peters.

design, deployment, and operations. It is critical to view mission-driven assessment as an on-going, evolving mechanism that allows the program to prioritize cyber capabilities in terms of mission requirements. This involves an on-going assessment beginning in early concept phases for a program and includes²⁷:

1. Characterization of the mission and system; for example, establishment of “Mission Measures of Effectiveness” to be applied.
2. Description of the relationship between the information being assured and the achievement of mission objectives; for example, creation/documentation of “Mission-Information Dependency Maps (MIDM)”. This includes an in-depth assessment of the potential impact from different *threat effects*, a fundamental shift away from the traditional vulnerability-based decision-making.
3. Threat Analysis and Risk Assessment for various threat sources. ***It is critical to note that until specific threat sources are chosen, this approach is applicable well beyond cyber-based threats. Thus, using this approach would enable mission assurance measurement for the mission as a whole, not only for cyber.***
4. Mitigation assessment and ongoing risk management. In this case, it is necessary to employ a rolling, prioritized risk accounting approach, so that risks and mitigations can be re-visited to assess the possible unintended consequences of our own actions and the impact of adversary actions.

These mission-driven measurements, once established, have multiple applications throughout the system lifecycle, including resource investment prioritization, Course of Action assessment and trade-off analysis, input to mission-based operator alerts and interfaces, and exploration of what-if scenarios as new threat vectors emerge.

In general, the basics of mission-driven assessment are already required of programs (for example, in mandates to employ program protection planning) in order to effectively apply the Risk Management Framework (also see section 3.1.2.2 and Appendix A Risk Management Framework - Primer). This document calls upon the programs to build upon that mandate to allow major gains in mission resiliency by extending that mission focus to key cyber decisions throughout the lifecycle.

4.1.2 Access Understanding/Control

In response to the next mission assurance question – Who/What Can Affect Me? –Access Understanding and Control capabilities must be defined, tracked, and enabled. Access control, as defined here, is a logical extension of the program protection plans and controls currently required of our Space Systems; however, because of the scope and reach of cyber and associated threats, it extends beyond traditional definitions of program protection. Access control activities must include plans and procedures that govern/apply to the program while it is under development, as well as specification of access control functions that will in fact become part of the space system design. Our primary challenge under this area is to identify and determine the scope of potential access to our system components so that informed decisions can be made about how to invest resources to manage access and respond to potential threats. Areas of potential access span the system lifecycle and could include critical program information, access to developer systems and networks, system software and hardware in development, system software and hardware undergoing testing, access to test ranges and launch control capabilities, operational account access, and maintenance activities, including software updates.

Access Control calls for the programs to actively understand where and when they are granting access to system or mission components – beginning long before operations commence. It levies responsibility on

²⁷ Specific examples here are from CMMA.

developers to actively control the accesses they establish, and to intentionally manage those accesses. It further extends to the operational community to track and manage operations-based system access, including test, launch, and early orbit functions, maintenance and network accesses, etc.

Access control approaches should span personnel access during all phases, software and hardware assurance, including supply chain management, and facility access and control.

4.1.3 Instrumentation/Measurement/Trust

The final enabling area, Instrumentation/Measurement/Trust, involves equipping the mission support environment – including the Space Systems and specifically the Space Segments – with sufficient instrumentation to determine the current state of cyber operations and arrive at measurements that reflect that state. These capabilities are needed to address the question – How Will I Know What Is Happening? Adequately answering that question leads to the design of the appropriate situational awareness capabilities for operations, but has impact much earlier. Access Understanding/Control processes will contribute significantly to scoping the potential risk sources and will impact this enabler. Mission-Driven Assessment will establish the priorities for cyber protection and cyber mission assurance. Thus, we will measure and assess our cyber environments differently depending on the missions involved and the mission impact potential.

As all of the areas evolve, the goal is to identify mission risk areas, understand the indicators that would signify the transition of risks to actual problems/threats, and ensure that the system design and implementation will allow those indicators to be recognized.

The Instrumentation aspect focuses on determining HOW and WHERE indicators will be generated and monitored. Critical questions to address here will be:

- Given that my most critical information for mission success exists at place A in the system during time X in a mission, how would indicators be recognized that signal impending threats to that information that would have serious mission impacts?
- What sensors/analytics/algorithms/alerts would enable recognition of this?
- How will these be incorporated into the system design and deployment?

The Measurement aspect focuses on applying the Instrumentation to determine the actual state of operations. Critical questions addressed here will be:

- What data is needed to determine the current cyber state of the system?
- How will the existing instrumentation be used to affect this determination?
- How will we adjust/tune the response to potential mission risks according to ‘conditions in the field’?

The Trust aspect focuses on the degree of certainty the Space System requires regarding the integrity of the hardware, software, applications, and operations. Technologies exist to increase the availability and integrity attestation for each of these. No area can be 100% attested to, but, in conjunction with Access Understanding/Control and Mission-Driven Assessment, priorities can be established and in turn will drive design requirements. Critical questions addressed here include:

- What level of assurance is required at each layer, given the highest risks to mission and the access available to my system?
- How do these requirements change over the course of the system lifecycle (e.g., identity management and trust may top priority during testing, when we necessarily have a wider set of

connections and exchanges occurring. After deployment, when accesses are better locked down, the integrity/trust we have in the cyber measurements of the flight software may be the highest priority?

- How will these trust levels be incorporated into system requirements and design?
- How will they be tested?

In total, this mission assurance enabling area must drive requirements early in the system lifecycle if there is to be any opportunity later to actively monitor/respond to cyber-based activity.

4.2 Information Assurance/Cyber Security Application Areas for Mission Assurance

While each of the enablers are critical, we cannot apply them towards achieving mission assurance unless we acknowledge them as necessary and *on-going* activities that evolve and adapt over the system lifecycle. As shown in Figure 4-3, we cannot simply do a paper assessment once and put it on a shelf. Each of the enablers should be treated as required functions that are part of a continuum of active mission assurance functions. However, despite using lifecycle terms, these applications of mission assurance capabilities should not be viewed solely as linear and chronologically-driven. Instead, these application areas should be viewed as an ongoing cycle of refinements driven by the emerging changes in the cyber environment – changes created by our own efforts, those of our adversaries, and those of neutral third parties.

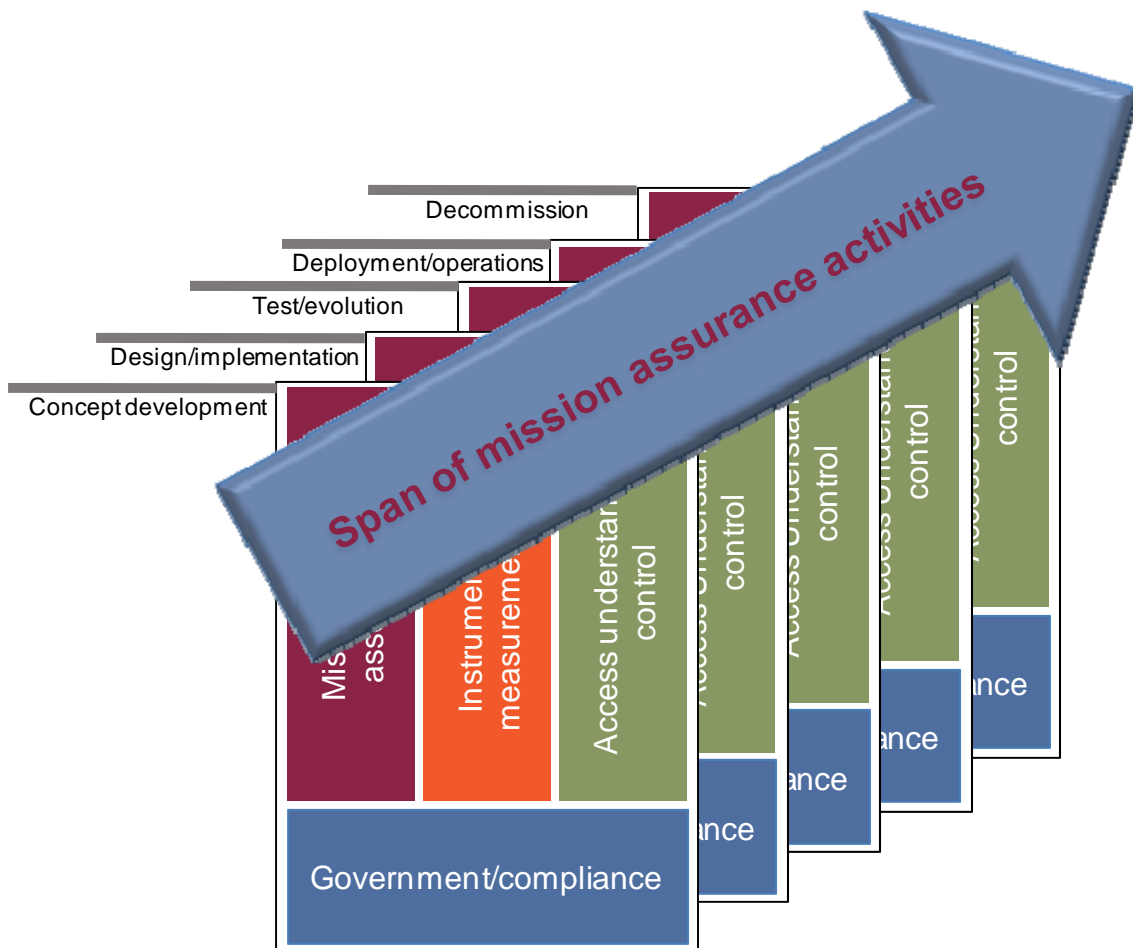


Figure 4-1. Cyber mission assurance must span lifecycle.

For new programs, efforts should begin with Concept Development, but extend through Design/Implementation, Test/Evaluation, Deployment/Operations, and Decommissioning. Each of the participants will have roles to play in each of those phases – and active Access Understanding/Control, Instrumentation/Measurement/Trust, and Mission-Driven Assessment tasks for them exist in every phase.

For existing Space Systems, the framework can and should be scaled to adapt to the reality of resourcing available to the program; however, it should not be rejected for legacy systems. In particular, the Access Understanding/Control and Mission-Driven Assessment functions could be applied to identifying process or operations-based mitigations to emerging threats and contributing to informed prioritization of limited operations and maintenance budgets.

4.3 Information Assurance/Cyber Security *Participants* for Mission Assurance

Cyber security today is treated as a separate discipline or an isolated series of milestones related to certification and accreditation. In fact, to achieve a cyber-ready mission assurance framework, the roles of each of the following participants – in each phase of the system lifecycle – must be considered and reassessed for the role they play and the responsibilities they bear. The participants include:

- Program/Acquisition Offices – The government offices invested with the responsibility of specifying and acquiring capabilities, and accepting solutions on behalf of the government.
- System Users – The operational community members whose missions depend upon the capabilities supplied by the system. These are not the personnel operating the space systems, but the end users executing operational missions that utilize the space systems.
- System Operators – The operational personnel that directly operate the space system components being developed and deployed, in support of the system users.
- Development/Integration Community – The design and development teams charged with supplying the specified capabilities. Typically these are contractor organizations that answer requests for proposal from the government and execute a contract to comply with government specifications. In addition to these contractors, however, this community may include separate integrator contractors, government integration teams, research labs and other capability providers, and government trusted agents (including Federally-Funded Research and Development Centers (FFRDCs) and University-Affiliated Research Centers (UARCs)).
- Test/Evaluation Community – The combined contractor, government, and service representatives responsible for providing test and evaluation environments, processes, tools, and events to validate, assess, and accept the capabilities for deployment, and to verify their utility throughout operations.

4.4 Integrated Framework for Cyber Mission Assurance in Space Systems

The overall guidance to the Space Systems community is to establish, resource, and maintain a cyber-ready mission assurance framework that encompasses each of the enablers in Section 4.1 and each of the application areas in Section 4.2. Table 4-1 captures this alignment. For each entry in the table, a corresponding guideline follows the table. The table entries provide a reference to those associated guidelines (e.g., GL 4-1 refers to Guideline 4-1 later in the chapter).

Table 4-1. Cyber Mission Assurance Framework Components

<p><i>CMA Enablers</i></p> <p><i>CMA Application Areas</i></p>	<p>Mission-Driven Assessment</p>	<p>Access Understanding/ Control</p>	<p>Instrumentation/ Measurement/ Trust</p>
<p>Concept Development</p>	<ul style="list-style-type: none"> • Perform Characterization - Define the measurements required to associate the cyber environment with the mission-to-information dependencies (GL 4-1) • Capture first order mission-to-information dependency mappings based on system concept (GL 4-1) • Prioritize mission risk areas for inclusion in solicitation (GL 4-1) • 	<ul style="list-style-type: none"> • Establish guidelines for documenting and tracking access control (GL 4-2) • Solicit community input to scope access requirements (GL 4-2) • Document access control requirements for solicitation (GL 4-2) 	<ul style="list-style-type: none"> • Use measurement and mission resilience characterization to prioritize compliance and governance (GL 4-3) • Create first iteration of the system <i>Trust Profile</i> required at each system component (GL 4-3)
<p>Design & Implementation</p>	<ul style="list-style-type: none"> • Refine MIDMs in accordance with updated PDR and CDR designs (GL 4-1) • Update program risk management plan with identified mission risks (GL 4-1) • Develop cyber situational awareness and mission readiness requirements driven by mission dependencies (GL 4-4) • Identify mission drivers for inclusion in user interface design (GL 4-4) 	<ul style="list-style-type: none"> • Expand access understanding to reflect development environment (GL 4-3) • Require developer accountability for corporate, subcontractor, and integrator access tracking (GL 4-2) • Derive requirements for any active access control features to be developed within system (GL 4-2) 	<ul style="list-style-type: none"> • Update Trust Profile at major program milestones (GL 4-3) • Derive instrumentation and measurement requirements (calculations and locations) based on access control and mission-driven assessment results (GL 4-3) • Design and implement mission-level readiness calculations based on trusted measurements (GL 4-3)

<i>CMA Enablers</i> <i>CMA Application Areas</i>	Mission-Driven Assessment	Access Understanding/ Control	Instrumentation/ Measurement/ Trust
Test & Evaluation	<ul style="list-style-type: none"> • Develop test cases that trace to the Mission Measures of Effectiveness and mission risk areas identified (GL 4-1) • Develop COAs associated with maintaining mission success factors (GL 4-5) 	<ul style="list-style-type: none"> • Activate test phase access control – account for security profile of all test connections (GL 4-2) • At completion of test, perform active removal of all test accesses (GL 4-2) 	<ul style="list-style-type: none"> • Test and verify trust profiles on periodic basis (GL 4-3) • Test and verify instrumentation and measurement (GL 4-3)
Deployment & Operations	<ul style="list-style-type: none"> • Calculate and provide to operator highest-interest drivers for mission success (GL 4-4) • Exercise mission-driven COAs and refine as needed (GL 4-5) • Periodically update MIDMs and mission risk prioritization based on threat conditions (GL 4-1) 	<ul style="list-style-type: none"> • Enable periodic review of operational accesses (GL 4-2) • Require automatic expiration of user and network connections (GL 4-2) • Identify and activate specific L&EO access control (GL 4-2) • At completion, perform active removal of L&EO accesses (GL 4-2) • Require periodic update of access profiles (GL 4-2) 	<ul style="list-style-type: none"> • Adjust/tune measurement profile based upon current operational state (Threat Condition, INFOCON, Mission Operations, etc.) (GL 4-3)

4.5 Guidance

The framework of capabilities and applications for cyber mission assurance presented in this section can be translated into the following guidelines. The detailed guidance specific to NSS-S systems and functionality are captured in subsequent chapters, but are directly related to the guidelines captured here.

<p>Guideline 4-1. Perform Mission-Driven Analysis to determine mission-information dependencies</p>
<p>Recommendation: Perform a mission-driven analysis that includes effects-driven assessment of the places where mission success is most dependent upon information exchanges supported via cyber.</p>
<p>Evaluation Criteria: <i>Full satisfaction of this guideline will require extension to current policy, programmatic, and practice. This should be actively sought. In the interim, however, it is still possible to achieve steps towards the intent of this guideline. These specific guidelines are found in the following sections. See Guidelines 5-2, 6-14, 6-17, 7-9.</i></p>
<p>Milestone: <i>Pre-acquisition (in DOD terms, pre-MDD). To be maintained and updated at appropriate occasions throughout the SDLC.</i></p>
<p>Rationale: Mission assurance in the face of cyber attack requires the ability to prioritize investments, information, and operational courses of action according to the greatest potential impact to mission success.</p>
<p>Stakeholders/Actions: Achieving this guideline will require action on the part of the following participants.</p> <p><u>Program Office</u></p> <ul style="list-style-type: none"> • Conduct baseline Mission-Driven Assessment on the program during the Concept Development phase, to include a list of candidate mission information risk areas • Use derived mission-information dependencies and risk assessment to prioritize Risk management Framework controls, identifying the controls that correlate to the highest priority mission information risk areas. Include priorities as government-furnished information • Program for on-going refinement and reassessment throughout the lifecycle – update assessment at each program milestone • Establish functional requirements for mission-based measurement and user interfaces <p><u>System Users</u></p> <ul style="list-style-type: none"> • Participate in Mission-Driven Assessment, to include assisting in Measure of Effectiveness selection, mission impact assessment, and mitigation evaluation <p><u>System Operators</u></p> <ul style="list-style-type: none"> • Participate in Mission-Driven Assessment, to include assisting in Measure of Effectiveness selection, mission impact assessment, and mitigation evaluation <p><u>Developer/Integrator</u></p> <ul style="list-style-type: none"> • Develop implementation requirements and approach that meet mission-based measurement and user interfaces requirements • Refine design approach following milestone reviews, documenting how highest priority mission information risk items are addressed in the design • Prepare transition report identifying mission information risk areas that will be unaddressed upon delivery to the government <p><u>Test/Evaluation Community</u></p> <ul style="list-style-type: none"> • Participate in Mission-Driven Assessment, to include assisting in Measure of Effectiveness selection, mission impact assessment, and mitigation evaluation. Incorporate the MDA results into test/evaluation planning to include test environment configuration, test scenarios, and high priority mission operations primary and secondary execution

Guideline 4-2. Establish and Implement Access Control functions across system lifecycle.

Recommendation: Create the programmatic processes, requirements, and organizational infrastructure to begin tracking Access Control information and using that information to guide system implementation, risk management, and operations.

Evaluation Criteria: *Full satisfaction of this guideline will require extension to current policy, programmatic, and practice. This should be actively sought. In the interim, however, it is still possible to achieve steps towards the intent of this guideline. These specific guidelines are found in the following sections. See Guidelines 5-2, 6-12, 6-13, 6-15, and 7-2.*

Milestone: *Pre-acquisition (in DOD terms, pre-MDD). To be maintained and updated at appropriate occasions throughout the SDLC.*

Rationale: Access Understanding/Control is required across system lifecycle to manage understanding of risk and identify mitigation points. Unmanaged access control during early program phases represents significant jeopardy to current programs.

Stakeholders/Actions: Achieving this guideline will require action on the part of the following participants.

Program Office

- Establish guidelines and program plan for documenting and tracking access control across the lifecycle
- Oversee Access Understanding/Control functions throughout lifecycle. Administer Access Control management functions retained by the government
- Solicit community stakeholders (system users, system operators, test/evaluation community) to participate in access control definitions prior to solicitation
- Generate requirements for development contractor to incorporate the Access Control functions into the system development processes
- Define functional requirements for any automated access control management capabilities

System Users

- Provide input on access needs to provide early influence on system capabilities
- Review/refine access profiles and requirements
- Maintain awareness of AU/C process – update Program Office if access needs or actual access configurations change

System Operators

- Provide input on access needs to provide early influence on system capabilities
- Review/refine access profiles and requirements
- Maintain awareness of AU/C process – update Program Office if access needs or actual access configurations change

Developer/ Integrator

- Provide Access Control approach in response to solicitation
- Administer Access Control management functions assigned by the government
- Assume accountability for Access Control management for duration of development phase, and encompassing all subcontractors, vendors, business systems, tools
- Maintain awareness of AU/C process – update Program Office if access needs or actual access configurations change

Test/Evaluation Community

- Provide input on access needs to provide early influence on system capabilities
- Review/refine access profiles and requirements
- Maintain awareness of AU/C process – update Program Office if access needs or actual access configurations change

<p>Guideline 4-3. Develop measurement plan and associated instrumentation approach</p> <p>Recommendation: Establish a cyber measurement plan that clearly traces instrumented feeds from the cyber environment through aggregation to association with mission outcome and potential impact to mission outcome.</p>
<p>Evaluation Criteria: <i>Full satisfaction of this guideline will require extension to current policy, programmatic, and practice. This should be actively sought. In the interim, however, it is still possible to achieve steps towards the intent of this guideline. These specific guidelines are found in the following sections. See Guidelines 5-2, 6-16, 6-17, 7-9.</i></p>
<p>Milestone: <i>Pre-acquisition (in DOD terms, pre-MDD). To be maintained and updated at appropriate occasions throughout the SDLC.</i></p>
<p>Rationale: A hierarchy of mission measurements decomposed into measurable cyber feeds forms the basis of instrumentation, situational awareness, and course of action decision support capabilities in the future. A trusted computing environment is a necessary precondition for cyber mission assurance (CMA), allowing the assumption of a higher integrity in the measurements of cyber state and the subsequent calculation of potential impact to mission outcome.</p>
<p>Stakeholders/Actions: Achieving this guideline will require action on the part of the following participants.</p> <p><u>Program Office</u></p> <ul style="list-style-type: none"> • Define trust profiles, derived from a mission-based analysis, to include trust requirements for hardware, operating systems, networks, identity, and applications. Include program plan for documenting and maintaining trust profiles throughout the lifecycle • Establish requirement for a measurement/instrumentation approach in contract solicitation. • Define functional requirements for measurement/instrumentation capabilities to be performed within system operations (Assurance level requirements, active vs. passive monitoring, operational automation, etc.) <p><u>System Users</u></p> <ul style="list-style-type: none"> • Participate in mission-driven assessment that in turn drives the definition of Measurement/Instrumentation requirements, including trust profiles <p><u>System Operators</u></p> <ul style="list-style-type: none"> • Participate in mission-driven assessment that in turn drives the definition of Measurement/Instrumentation requirements, including trust profiles <p><u>Developer/Integrator</u></p> <ul style="list-style-type: none"> • Derive detailed requirements and approach for review for concurrence at PDR and CDR • When Developing the Integrating Capabilities: Develop a system Measurement/Instrumentation approach as part of the system design that clearly traces instrumented feeds from the cyber environment through aggregation to association with mission outcome and potential impact to mission outcome • When Developing Supporting/Interfacing Capabilities: Develop a system Measurement/Instrumentation approach that clearly provides required instrumentation or measurement feeds to support integrating capability's ability to determine association with mission outcome and potential impact to mission outcome <p><u>Test/Evaluation Community</u></p> <ul style="list-style-type: none"> • Develop and apply test facilities and test cases that validate the required Measurement/Instrumentation capabilities, as well as the required trust profile capabilities

Guideline 4-4. Require Mission-based Cyber Situational Awareness

Recommendation: Establish programmatic requirements to define Cyber Situational Awareness feeds that will leverage the measurement profiles already calculated and enable display of situational awareness in terms of potential impact to mission success.

Evaluation Criteria: *Full satisfaction of this guideline will require extension to current policy, programmatic, and practice. This should be actively sought. In the interim, however, it is still possible to achieve steps towards the intent of this guideline. These specific guidelines are found in the following sections. See Guidelines 5-2, 6-18, 7-8.*

Milestone: *Pre-acquisition (in DOD terms, pre-MDD). To be maintained and updated at appropriate occasions throughout the SDLC.*

Rationale: Cyber mission assurance requires that the operators (spacecraft, system, and mission owners) are provided cyber status in a format that permits determination of potential impact to mission outcome.

Stakeholders/Actions: Achieving this guideline will require action on the part of the following participants.

Program Office

- Coordinate with operational community to establish a mission concept for Cyber Situational Awareness that aligns with the Mission-Driven Assessment.
- Define the functional requirements needed to achieve the Cyber Situational Awareness mission concept
- Establish programmatic requirements to define Cyber Situational Awareness feeds that will leverage the measurement profiles already calculated and enable display of situational awareness in terms of potential impact to mission success.

System Users

- Participate in requirements definition for Cyber Situational Awareness
- Assess system scenarios to provide input on mission impact that can be determined from the Cyber Situational Awareness available
- Incorporate cyber-based-risk scenarios into training and operational exercises. Ensure selected scenarios represent the high priority mission risk items.

System Operators

- Participate in requirements definition for Cyber Situational Awareness
- Define Tactics, Training, Procedures (TTPs) that incorporate Cyber Situational Awareness into overall system operations. Implement TTPs and associated Standard Operating Procedures
- Conduct cyber-specific training/operational exercises

System Network Operations/Cyber Personnel

- Participate in requirements definition for Cyber Situational Awareness
- Contribute to Tactics, Training, Procedures (TTPs) that utilize and apply the system's Cyber Situational Awareness capabilities. Implement TTPs and associated Standard Operating Procedures
- Conduct cyber-specific training/operational exercises
- Provide, to systems operators and system users during mission operations, expertise regarding implications of reported Cyber Situational Awareness

Developer/Integrator

- Develop operational requirements and design to implement the functional requirements for Cyber Situational Awareness
- Document Cyber Situational Awareness approach at PDR/CDR
- Refine and adapt Cyber Situational Awareness design approach following PDR/CDR

Test/Evaluation Community

- Design mission-based test cases to exercise Cyber Situational Awareness and underlying Measurement and Instrumentation feeds
- Participate in definition, coordination, and execution of tests and exercises that assess Cyber Situational Awareness capabilities across multiple, separately developed systems

Guideline 4-5. Require Mission-based Cyber Course of Action Development

Recommendation: Develop mission-based preplanned courses of action that leverage the mission-information dependencies derived during mission-based analysis.

Evaluation Criteria: *Full satisfaction of this guideline will require extension to current policy, programmatic, and practice. This should be actively sought. In the interim, however, it is still possible to achieve steps towards the intent of this guideline. These specific guidelines are found in the following sections. See Guidelines 5-2, 6-19, 7-9.*

Milestone: *Pre-acquisition (in DOD terms, pre-MDD). To be maintained and updated at appropriate occasions throughout the SDLC.*

Rationale: Cyber mission assurance requires that operational decisions regarding the cyber infrastructure are made in the context of potential impact to mission outcome. Further, the potential speed and scale of cyber impact due to attack requires a framework of preplanned courses of action that can be extended based on current conditions.

Stakeholders/Actions: Achieving this guideline will require action on the part of the following participants.

Program Office

- Coordinate with operational community to establish a mission concept for Mission-based Cyber Course of Action management (to include Initial Operational Capabilities, Full Operational Capabilities, and the flexibility for future expansions to be applied across multiple, separately developed systems).
- Define the functional requirements needed to achieve the Mission-based Cyber Course of Action management (which may range from only alerts from the Cyber Situational Awareness functions through automated cyber response – this will be program, mission, and threat condition-specific and will evolve over the lifetime of the mission)
- Develop Cyber Mission Resilience/Cyber Risk Response Concept of Operations at an appropriate level based on the results of the baseline Mission-Driven Assessment. Refine following MDA update (which occur following program milestones)

System Users

- Contribute to defining Cyber COA management operations concept
- Contribute to Tactics, Training, Procedures (TTPs) that align with the defined Cyber COAs
- Incorporate cyber-based-risk scenarios into training and operational exercises. Ensure selected scenarios represent the high priority mission risk items.

System Operators

- Contribute to defining Cyber COA management operations concept
- Define Tactics, Training, Procedures (TTPs) that align with the defined Cyber COAs
- Implement TTPs and associated Standard Operating Procedures
- Conduct cyber-specific training/operational exercises

System Network Operations/Cyber Personnel

- Contribute to defining Cyber COA management operations concept
- Contribute to Tactics, Training, Procedures (TTPs) that align with the defined Cyber COAs
- Implement TTPs and associated Standard Operating Procedures
- Conduct cyber-specific training/operational exercises

Developer/Integrator

- Develop operational requirements and design to implement the functional requirements for Cyber COA management (to include an adaptable user interface framework so future expansions can be applied across multiple, separately developed systems).
- Contribute to Tactics, Training, Procedures (TTPs) that align with the defined Cyber COAs, specifically regarding expected system performance and capabilities

Test/Evaluation Community

- Develop and apply test facilities and test cases that validate the required Cyber COA management capabilities
- Participate in definition, coordination, and execution of tests and exercises that assess Cyber COA management capabilities across multiple, separately developed systems

5. National Space System Acquisition Guidance

The risk-management approach of information systems described in chapter 3 is most effective when integrated into the system development lifecycle (SDLC). In addition, establishing a cyber mission assurance framework as described in chapter 4 requires the necessary measures, as outlined in that chapter's guidelines, to be reflected in the acquisition process and folded into program execution. As such, the system acquisition process will have to ensure that IA risk management is an integral part of system definition, development, and operation. Given that the primary goal of the acquisition process is to successfully deliver within cost and on-schedule an operational system that meets its mission goals, including *IA risk management* (risk management practices that address IA issues) as part of mission assurance is of paramount importance to meeting mission goals. The challenge for the acquisition process is to effectively achieve this goal while balancing cost, schedule, and overall development risk. The goal of this chapter is to provide specific acquisition guidance that will help in achieving successful integration for Space Segment programs.

This chapter recognizes that Space Segment acquisition of capabilities sometimes will occur as part of new program starts, and other times will incrementally build on existing or legacy capabilities and programs. The challenges for IA risk management will necessarily differ among the two. New program starts afford an opportunity for the definition of the system security architecture as part of the system definition phase of the program. On the other hand, existing systems that are being upgraded or augmented with new mission capabilities will have to accommodate IA risk management within their existing security architecture while managing the IA risk for the new capabilities.

Maximizing Information Security while minimizing program risk/cost is a balancing act for the acquisition organization. It involves evaluating IA risk/cost against the impact of IA protective measures on program risk and cost. This balance can only be achieved through the involvement of multiple stakeholders including the following:

- The overseeing acquisition organization responsible for the overall definition and delivery of the Space Segment capabilities
- The Space Segment Contractor(s), or potential contractor(s) in the competitive phase of the program
- The User Segment, which encompasses both the system components developed for the end users of the mission capabilities, as well as the end users themselves
- National security organizations which are responsible for setting security policy and evaluation of security implementations
- The Authorizing Official (AO) [In DOD, the Designated Approval Authority (DAA)], which has the ultimate responsibility of providing or withholding the system's authority to operate

The guidance offered in this document will attempt to facilitate a process of stakeholder involvement under existing security policy and best practices within the applicable governance discussed in chapter 3 and the cyber mission assurance framework of chapter 4. With appropriate stakeholder involvement, the acquisition organization is better able to integrate IA risk management into the program baseline throughout the acquisition life-cycle, while balancing program execution cost and risk.

5.1 Trends in National Space Acquisition

The field of Information Assurance and Cyber Security has been rapidly evolving over the last decade. Changes stemming from net centricity and the evolving cyber threats have lead to new security policies, directives, and instructions aiming at providing a stronger security posture for

government systems and networks. Most of these IA policies, directives and instructions provide high level guidance, for Information Systems, and do not necessarily provide requirement flow down to specific IA controls and technical requirements on a space program. The rapid evolution and high level nature of guidance thus presents a challenge to the acquisition of new capabilities on Space Segment systems where the SDLC is much longer than typical SDLC on ground based systems. This challenge can be met partly through the robust application of the ISSE as further discussed in the development chapter of this report.

One factor compounding the System Engineering challenge of IA requirement flow-down and the associated acquisition implications of security-related requirements is the lack of participation from all stakeholders, especially in the early stages of system definition. Typically, the application of the ISSE is left to the system contractor working with their acquisition organization technical interface. Participation from other key stakeholders such as the user segment, National Security organizations, and the AO, is often hindered by resource availability. This could be the result of funding constraints or the unavailability of Space Segment specific specialized resources within the stakeholder organization. In addition, the low level of technical maturity of the IA system architecture in the early stages of system definition contributes to the lack of stakeholder interest and participation.

Another factor to consider in the acquisition of NSS-S systems is the need for a better common understanding among stakeholders of the system security risk-benefit equation which will eventually drive the system definition and implementation. The following factors are typically more valued by some of the stakeholders and less by others, thus a common understanding of them is needed:

- Potential system security threats are typically not well understood by the contractor and the technical acquisition organization.
- Cost/risk impact of security controls are typically not well understood by stakeholders outside of the contractor and technical acquisition organization.
- The system security posture and its technical capability to mitigate security risk are generally confined to the contractor, especially on existing or legacy system security architectures.
- The impact of security controls on user mission and operations are not always appreciated by all stakeholders.
- Conversely, the potential impact of security vulnerabilities on system operation and mission utility, as well as other interconnected systems and networks, is not always appreciated by the user segment.

Finally, emerging technology trends in space systems – which could enable or enhance the cyber threat compared to early space system implementations – add to the acquisition challenge. While these emerging technology trends hold the promise for enhanced mission capabilities, their security implications have not yet been fully evaluated and understood. Enhanced space architectures include multifunctional platforms, hosted payloads, networked payloads, small and micro satellite and satellite clusters, and space-to-air, and space-to-ground architectures. These emerging space technology trends introduce complex security issues such as user data protection while in transit, network interconnectivity, space domain separation, and information security boundary definition.

5.2 National Space Segment Acquisition Roles and Responsibilities

Chapter 3 of this document identified applicable IA governance, standards, and guidance for National Space. This chapter will attempt to identify the stakeholders as per the governance in chapter 3 for National Space acquisition programs. Many examples in this chapter will be based on DOD systems, policies and standards, however many of the stakeholders identified here, or equivalents, will be involved in IC acquisition programs.

At the highest policy level, the office of the Under Secretary of Defense for Acquisition, Technology and Logistics, USD(AT&L), serves as milestone decision authority (MDA), and conducts independent evaluation of performance and resource requirements and approves program milestones. The National Security Agency (NSA), is responsible to plan, budget, and develop, programs to protect space systems. The NSA is also responsible for evaluating and certifying cryptography used in such systems, as well as performing end-to-end system security evaluations when requested. The Heads of the DOD Components are responsible for ensuring solicitations/contracts incorporate appropriate security and certification requirements and budget, and are ultimately responsible for validation of the requirements. Finally, Commander United States Strategic Command (CDRUSSTRATCOM) is responsible for assigning the system MAC level, Confidentiality Level, and naming an Authorizing Official (AO).

At the program execution level, we identify the following stakeholders, and their roles:

- User organizations whose role is to identify needed capabilities and mission requirements.
- The acquisition organization responsible for system procurement to meet mission capabilities, including requirements, budgets, contracts, etc. The acquisition organization is often supported by Federally Funded Research and Development Corporations (FFRDC) or System Engineering Technical Advisory (SETA) contractors.
- The contractor organization responsible for the development and delivery of the system to meet requirements derived for needed mission capabilities.
- NSA responsible for security evaluation and crypto certification.
- AO which is responsible for granting system ATO.

Specific roles and responsibilities for the successful integration of IA risk management in program mission assurance will be presented in the next section.

5.3 Programmatic Guidance

The following programmatic guidance focuses on stakeholder collaboration to provide program specific solutions to meeting security policy. By viewing IA in the context of a risk management process under mission assurance, the guidance attempts to facilitate a risk-benefit process, and ensure any residual security risk is acceptable for the purpose of achieving system ATO. Most of this guidance applies to new program starts as well as new capability insertion on existing systems/ programs. Specific guidance will also be given for capability insertion programs. This guidance is programmatic in nature. Development guidance is provided in chapter 6.

Attention to program protection (P2) is an essential programmatic requirement to achieve mission resilience. P2 is an umbrella concept with three sub-elements: Mission Protection, System Security Engineering (SSE) and Personnel and Facility Security Management.

Program Protection (P2). The safeguarding of defense systems and technical data (critical program information) anywhere in the acquisition process, to include the technologies being developed, the support systems (e.g., test and simulation equipment), and research data with military applications. This protection activity involves integrating all security disciplines, counterintelligence, and other defensive methods to protect the essential program information, technologies, components and systems data from intelligence collection and unauthorized disclosure²⁸. Enhanced P2 (cf., Guideline 4-1 and Guideline 4-2) should integrate Mission, System, and Operations.

²⁸ From: DOD 5200.1-M – Acquisition Systems Protection Program.

Mission Protection. The identification and analysis of program observables for the purpose of developing containment strategies to alter an adversary’s perception of the program’s activities, or to otherwise prevent an adversary from obtaining or deducing critical program information via function analysis.

System Security Engineering (SSE). An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities²⁹. Within SSE, there are relevant sub-specialties, including Information Assurance Systems Engineering (IASE) / Information System Security Engineering (ISSE). SSE and its sub-specialties incorporate a risk-based management approach.

Personnel and Facility Security Management. Includes physical identification, authentication and access control, information system security officers, etc. Security management, like information assurance, incorporates a risk-based approach.

5.3.1 Guidelines

<p>Guideline 5-1. Initiate enhanced Program Protection</p> <p>Recommendation: Based on current intelligence and technology assessments,</p> <ul style="list-style-type: none"> • determine key technology elements and information to be protected throughout the program; • plan for protecting those technologies and information; • protect those technologies and information throughout the program lifecycle.
<p>Evaluation Criteria: Stakeholder concurrence that important program information is adequately protected based on a sound Program Protection Plan (PPP) and periodic review of the adequacy of the PPP, and all program’s stakeholders’ effectiveness at meeting their obligations under the PPP.</p>
<p>Milestone: Beginning at concept development and continuing through solicitation response, and throughout program lifecycle.</p>
<p>Rationale: Protection of key technologies, components and information systems is necessary throughout the program lifecycle to prevent subversion of the information system and therefore its mission and mission information.</p>
<p>Stakeholders/Actions:</p> <ul style="list-style-type: none"> • Program Office: Establish program policy for information repository and program interchange protections by all program participants. Develop an initial Program Protection Plan (PPP) identifying critical program information (CPI) and technology components for mission success. Conduct periodic reviews of adequacy of all stakeholder PPP’s and effectiveness at meeting their protection obligations. Involve appropriate security technical representatives (e.g., AO, CA, NSA) in all PPP reviews, to assess likely effectiveness against the current threat environment. • Developer: Update PPP, detailing planned implementation of the defined policy, information and technologies, to include lower tier subcontractors as required. Conduct program protection in accordance with planned implementation. Provide periodic updates to the developer PPP, and support periodic program office reviews of PPP implementation. • System Operator, User: Contribute mission operations perspective to PPP detailing planned implementation in the operational and user environments. Perform planned implementation, provide periodic updates to the operational PPP, support periodic AO representative and/or Program Office review of PPP implementation. Include contractors and vendors in PPP implementation as required.

²⁹ From: MIL-HDBK-1785: System Security Engineering Program Management Requirements

Guideline 5-2. National Space Program IA Integrated Product Team (IPT)

Recommendation: Establish a persistent collaborative institutional body with representation from all stakeholders and responsibilities as outlined below. The usual name for this kind of institutional body is an Integrated Product Team (IPT); this name is used herein.

Evaluation Criteria: IA IPT active in all stages of acquisition cycle.

Milestone: All

Rationale: IA IPT provides venue to manage IA risk

Stakeholders/Actions: The IA IPT should be established by the Acquisition Organization/Program Office, and should include representation of the following stakeholders at a minimum, with responsibilities as outlined below:

- Acquisition Organization/Program Office: Chair IPT. Product responsibility to provide Program Manager with recommendations on IA controls specific to space program which balance preventive measures against program execution. Engage IA subject matter experts from the FFRDC, UARC, and SETA support team. Evaluate programmatic impact of IA controls. Provide approval of IA requirement flow down by contractor. To the extent feasible, and with the help of other IPT stakeholders, instigates, leads and flows down into requirements the Cyber Mission Assurance guidance from section 4.
- AO: Evaluate system security posture including residual risk. Evaluate applicability of threats to space system. Provide close tie between requirement set and achieving system ATO. Evaluate contractor implementation plan of IA controls and security requirement flow down.
- National security organization: Provide policy and implementation guidance. Provide threat analysis. Provide system vulnerability analysis including specific application of potential threats to program capabilities. Evaluate certification and accreditation approach.
- Contractor: Provide DIACAP Implementation Plan (DIP) for DOD systems (or equivalent for IC or Civil Government systems) including tailoring of preventive measures to space system. Provide requirement flow-down from DIP. Provide impact analysis of IA requirements. Provide C&A approach. Provide IA risk management plan and early IA risk reduction activity. Implements Cyber Mission Assurance requirements derived from the guidance of section 4 to provide access understanding and control, instrumentation and measurement, and the mission driven assessment.
- User segment: Evaluate impact of IA controls on system operations and user mission capability.

Guideline 5-3. IA Risk Management Integration in Program Milestones

Recommendation: Integrate IA risk management in all system milestones, beginning with Initial Capability Determination (ICD) and Material Solution Analysis through system Initial Operating Capability.

Evaluation Criteria: Identification of security requirements in the early stages of the acquisition, followed by system security assessment and evaluation throughout the rest of the acquisition lifecycle, are reflected in existing program milestones and deliverables. Sound system security engineering, security risk reduction, and security operational controls and procedures are embedded throughout the lifecycle.

Milestone: Starting with pre-Milestone A activities, and continuing through all subsequent program milestones.

Rationale: Integration of IA risk management and IA controls with program milestones, including ICD, ensures funding for activity, application of System Engineering process, and efficiency in implementation, test and evaluation of IA controls.

Stakeholders/Actions: Acquisition organization should ensure IA risk management integration in all system milestones. National Security Space Acquisition policy identifies acquisition phases and milestones. IA risk management should be effectively incorporated in all phases of the acquisition cycle.

- This includes integration of sound system security engineering, security risk reduction, and security operational controls and procedures, as part of the overall system design, development, and operation. Such integration will not only mitigate security threats to the system, but also mitigate program risk and ensure mission success.
- It also includes identification of security requirements in the early stages of the acquisition, followed by system security assessment and evaluation during the acquisition phases of the program, consistent with system maturity. This will provide the best approach towards successful system certification and accreditation.

IA risk management can be effectively incorporated in all phases of the acquisition cycle. Integration of sound system security engineering, security risk reduction, and security operational controls and procedures, as part of the overall system design, development, and operation will not only mitigate security threats to the system, but also mitigate program risk and ensure mission success. Identification of security requirements in the early stages of the acquisition, followed by system security assessment and evaluation during the acquisition phases of the program, consistent with system maturity, provides the best approach towards successful system certification and accreditation.

Guideline 5-4. New Capability Insertion on Existing Programs

Recommendation: Evaluate security architecture of existing system and determine applicability of security policy to new capabilities.

Evaluation Criteria: Evaluation conducted as part of Materiel Development Decision (MDD)

Milestone: MDD; other milestones as applicable.

Rationale: Existing systems under consideration for insertion of new capabilities have to accommodate IA risk management within their existing security architecture while managing the IA risk for new capabilities. While there is currently little guidance on adding new capabilities to existing systems, DTM-09-025 recognizes the need for the acquisition organization to conduct an evaluation as part of the MDD for new capabilities to determine the proper entry phase of the acquisition cycle for new capabilities. Including a security evaluation as part of the MDD evaluation, will allow the acquisition organization to better integrate IA risk management as applicable to the acquisition phase of the new capability insertion.

Stakeholders/Actions: Acquisition organization should evaluate security architecture of existing system and determine applicability of security policy to new capabilities based on guidance in Directive-Type Memorandum (DTM) 09-025 – Space Systems Acquisition Policy (SSAP)³⁰

- This evaluation will consider new IA requirements and address any IA risk precipitated by the existing security architecture of the system.
- The evaluation will result in recommendations on how to integrate IA risk management within the overall risk management framework for the program.

5.4 Acquisition Relationship to Governance and Standards Guidance

As discussed in chapter 3, successful program acquisition will have to be cognizant of the evolving standards and governance as recommended in Guideline 1. Establishing a program IA IPT or similar structure to ensure key stakeholder participation will enable program exposure to the evolving IA landscape, as well as stakeholder agreement on how to impact the acquisition process in response to such evolution. Integration of IA risk management into system acquisition will provide the vehicle to translate governance into mission capabilities and incorporate the needed IA controls using a low risk system engineering-based approach.

5.5 Acquisition Relationship to Cyber Mission Assurance Framework Guidance

The three tenets of establishing a cyber mission assurance framework as discussed in chapter 4 of this report center around the following:

1. Access understanding and control
2. Instrumentation and measurement
3. Mission driven assessment

All three are closely tied to the acquisition process as discussed in this section, and are, in fact, enabled by the implementation of the acquisition guidance outlined here. Program protection planning

³⁰ Directive-Type Memorandum DTM-09-025, issued by the Undersecretary of Defense for Acquisition, Technology, and Logistics, dated Oct 18, 2010.

(Guideline 5-1) establishes access understanding and needed control. Prioritization of compliance and governance based on mission characterization and measurement will be performed by the acquisition stakeholders. The incorporation of needed instrumentation and controls to enable continued situational awareness throughout the development and operation lifecycle is facilitated by the integration of IA risk management into the system baseline. Mission driven assessments can be incorporated into the acquisition organization evaluation of the system security architecture and mission capabilities for both existing and new-start systems.

6. National Space System Update & Development Guidance

The development phase for capability upgrades for existing systems and particularly for new systems is rich with guidance and requirements for Information Assurance (IA). These IA requirements, as commonly implemented, provide a necessary baseline for securing systems against cyber attack, but are generally insufficient to provide mission resilience against the advanced cyber threat. IA requirements that are commonly implemented well among the NSS-S community are not repeated here, although selected high-level specifications are provided for reference. The development guidance provided in this chapter consists of needed enhancements to common practice, when implementing existing IA requirements, as well as more detailed guidance for the development community in implementing the mission resilience guidelines of chapter 4, *Establishing a Cyber Mission Assurance Framework*. The combination of enhanced implementation of existing IA requirements with mission resilience guidelines should effectively harden National Security Space (NSS-S) systems against the advanced cyber threat. Analogous to radiation-hardening this “cyber-hardening” will impact the design and design processes of many NSS-S system components but is necessary for mission resilience in the face of today’s hostile cyber security environment.

6.1 General Guidance

TOR-2009(1455)-6³¹ provides excellent motivation and general guidelines for hardening of NSS-S systems against the advanced cyber threat, and is recommended as an important resource to guide NSS-S ground upgrades and development programs. This section leverages TOR-2009(1455)-6 for identification of weaknesses that are likely common to NSS-S program developments, attempts to enumerate specific guidelines for accomplishing the goals of that TOR in those areas, then adds guidelines in conjunction with the mission resilience goals of chapter 4. Since many programs which might benefit from this guidance are already in operation or well into development, this guidance addresses both existing and new development programs. Existing programs may well have met the intent of some recommendations but should pay particular attention to those guidelines tagged for updates throughout the program lifecycle. New programs should address all of the recommendations and provide a high-level implementation plan or rationale for recommendations they deem not applicable as part of their system security planning documentation. Guidelines for protection of particularly sensitive or mission critical information are tagged with (OBJ), whereas untagged guidelines should be required throughout NSS-S systems or rationale provided for their non-applicability.

Guidelines within this chapter use the common structure for this document but may be better understood within the following specific context for this section:

- The System Security Management Plan (or similar document) will normally be used to capture overall IA and Cyber Security Architectures, process and design approaches for current security practice as well as for the following development recommendations.
- Evaluation criteria provide specific information to help the reader more precisely understand the intent of the recommendation.
- Milestones are all within the development cycle (of a system update or new start) so generally refer to development cycle system level design reviews.
- Rationale provides the motivation for the recommendation so provides the system, or enterprise intent and objective for the recommendation.

³¹ TOR-2009(1455)-6, Advanced Cyber Threats to Satellite Communication Programs

- Stakeholders listed will include those with active input or responsibility for a specific guideline. Exceptions to the following general stakeholders responsibilities will be included in the specific applicable recommendation:
 - Authorizing Official (AO) – government official with the authority to formally assume responsibility for operating a system at an acceptable level of risk, generically responsible for the adequacy of security controls, will only be consulted for unusual requirements or scenarios during development. Will be responsible to review certification artifacts and making a risk assessment prior to allowing, or disallowing system operations.
 - Certification Authority (CA) – senior official having the authority and responsibility for the certification of information systems governed by a component IA program, certified IA components and controls will be part of the larger system to be approved by the AO.
 - System User – end user of the system functionality, whose input will be sought for implementation of requirements that impact the end user’s experience or interactions with the system (e.g., for NSS-S systems a consumer of sensor information or user of a satellite communications terminal).
 - System Operator – personnel who maintain, administer, and operate system equipment to enable it providing functionality to system users (e.g., satellite or network operations personnel).
 - Program Office – government procurement agency for development of new functionality or systems, responsible to ensure all needed functionality is provided.
 - Developer – contractor tasked with developing, implementing, testing and delivering system functionality; often used to refer to the Prime Contractor/Integrator, but most generally also refers to subcontractors, and vendors.
 - Subcontractor or vendor – lower tier contractors employed by the Prime Contractor for specific elements or components within the system.

6.1.1 NSS-S Information Assurance Systems Engineering

All NSS-S, including the entire space segment must have the underpinning of solid IA system engineering, first for the procurement activity Program Office and the System Engineering and Integration (SE&I) activities per TOR-2010(8507)-7³², as updated in the IA chapter of the most recent Mission Assurance Guide (MAG), TOR-2007(8546)-6018, REV A.

Secondly, the developed system must have adequate IA controls for a high-value NSS-S system applied to both ground and space based components. Tailoring those controls designed for ground systems to space-based components was historically considered unnecessary as the space components were isolated and considered effectively protected by their individual “stove-pipe”. However, with increased network access to the command and control of some of those systems, including some payload control from user terminals, the protection afforded by the stove-pipe assumption is no longer valid, and rigorous IA controls must be applied to space components.

Guidance for IA controls (e.g., DOD 8500.2, SP 800-53) is generally written for application to ground systems (i.e., computers, networks, etc.). Consequently, these IA controls are not easily translated for application to space systems, particularly for space vehicle and payloads. For DOD systems, with DOD 8500.2 imposed, TOR-2007(8583)-6702³³ provides guidance on selection and

³² TOR-2010(8506)-7, Information Assurance: An Integral Component of Mission Assurance, as updated in the IA chapter of the most recent Mission Assurance Guide (MAG), TOR-2007(8546)-6018, REV A

³³ TOR-2007(8583)-6702, Information Assurance Handbook for DOD Space Systems: Guidance on Application of DOD 8500.1/8500.2 IA Controls

application of the DOD8500.2 controls for space systems and should be used as a starting point for deriving Space System IA Requirements from the 8500.2 IA Controls. For systems implementing NIST SP 800-53 controls, a successor to the 8500.2 Space-application TOR is currently under development at The Aerospace Corporation; if available, it should be used. If that document is not available the referenced 8500.2 application guide will still be of benefit by cross-referencing controls. As with other government requirement source document, IA system requirements derived from the applicable IA control per NIST SP 800-53 or DOD8500.2 are assumed to be flowed down to the appropriate hardware and software components for implementation as part of the standard system engineering process.

<p>Guideline 6-1. Allocate IA requirements, goals and objectives down to components</p> <p>Recommendation:</p> <ul style="list-style-type: none"> • Leverage TOR-2007(8583)-6702 (or its successors) to allocate and assign IA requirements, goals and objectives through the hierarchy of applicable elements (e.g., space vehicle, payload module, processor SW component, ground control user interface). • Ensure that allocated requirements, goals, and objectives are allocated and verified whether to an in-house, subcontractor or vendor element or component.
<p>Evaluation Criteria: Stakeholder approval of requirements, goals, objectives, and verification approach and verification data as allocated to each applicable element.</p>
<p>Milestone: Milestone A, Milestone B, and major design reviews during system acquisition and capability updates</p>
<p>Rationale: Important IA considerations are often not considered and incorporated into the system concept and design early enough to be done economically or effectively, additionally even when considered they may not be communicated effectively to the appropriate implementer or verified in the vendor product, component or subsystem.</p>
<p>Stakeholders/Actions:</p> <ul style="list-style-type: none"> • System Operator should provide input through all design stages so that IA features do not unnecessarily interfere with the mission or system operations. • Program Office must assure that appropriate IA requirements, goals, and objectives are included in the procurement package, effectively implemented by the developer and procedurally supported and maintained during operations. • Developer must incorporate IA considerations in the basic system architecture, then implement and verify effective operation of the IA measures as part of system certification. • Certifying authority must validate that appropriate IA measures are included in the system concept and then verify their proper implementation.

6.1.2 NSS-S Ground Enclave Mission Assurance

Since NSS-S ground enclaves are the normal entry point to the high-value space-based assets, ground components require careful cyber-hardening to assure availability of the space asset. As an essential baseline all ground enclaves must incorporate applicable IA controls (e.g., DOD 8500.2, SP 800-53) and be certified and accredited per their governing policy (e.g., ICD-503, DOD 8510 or NIST SP 800-37). As the controlling system element for the space-based element, the satellite operation ground element capabilities will necessarily be heavily involved in providing capabilities for incorporating the guidance for space components in section 6.2. Additionally, depending on system architectures, all NSS-S ground components may need to participate in the system hardening guidance of section

6.2.2. However, specific to ground enclave components is the need to ensure that all network interconnections are identified and controlled per Guideline 6-2.

<p>Guideline 6-2. Provide technical capability to continuously secure all ground enclave interconnects</p> <p>Recommendation:</p> <ul style="list-style-type: none"> • Implement measures to continuously monitor for new network connections. • Document all design/implementation time ground enclave interconnections • Provide means to secure interconnections per applicable policy.
<p>Evaluation Criteria: System interconnects have a certified cross domain solution for connections to enclaves not accredited to the policy of the system in question, or the connected system must be accredited to the subject system policy. System is routinely scanned for new network connections, to include: remote login, wireless, maintenance and factory support. Unauthorized connections may be terminated with operator approval and appropriate corrective action taken.</p>
<p>Milestone: System acquisition and capability updates</p>
<p>Rationale: Ground enclaves often end up with undocumented and improperly secured connections exposing NSS-S systems to the broad spectrum of cyber threats. These spurious connections may result from: system troubleshooting, system maintenance, improper configurations, user error or deliberate hostile action. Since these connections have the effect of bypassing the system’s security design, the system becomes exposed to unauthorized access, malware and exploitation.</p>
<p>Stakeholders/Actions:</p> <ul style="list-style-type: none"> • System Operator should provide input through all design stages so that implemented capabilities can be used appropriately to achieve continuous monitoring for new network interconnects and securing them. • Program Office must assure that requirements for continuous monitoring capabilities and means to secure discovered interconnects are in place before development. • Developer must provide system capabilities meeting the requirements and enabling continuous monitoring for and securing of new network interconnections.

6.2 Addressing the Advanced Cyber Threat for NSS-Space Components

Since space-based components can no longer be assumed to be protected by a stove-piped architecture, the advanced cyber threat must also be addressed in space-based components or they can become the weak link in the enterprise regarding cyber threats. Consequently, the development processes, data protection, architecture, development, and implementation of the space components must also address the advanced cyber threat. Comparison of the cautiousness, analysis, and design practices of the space development community with that of the Type 1 crypto community reveals many similarities which are leveraged in the following recommendations for addressing the advanced cyber threat in space hardware and software. Section 6.3 is limited to specific recommendations for space hardware and software architecture and design.

6.2.1 Agility

Satellite functionality must adapt rapidly, and must be adapted over time, in response to unforeseen threatening circumstances in the environment (whether the physical or the cyber environment). Since there is a very real risk of losing all control or functionality of a satellite when making changes to its

operational software, updates tend to be infrequent, minimal, and carefully done. This tendency naturally limits the ability of the spacecraft software system to address unforeseen circumstance, increasing the window for vulnerability probing and attack development. In addition to the System Hardening recommendations of section 6.2.2 and the Enhanced Program Protection guidance of section 6.3.1, specific recommendations are provided, in Guideline 6-3 through Guideline 6-5 below, to reduce the risks associated with change of functionality, thereby enabling the needed degree of agility within space-based components of the system.

<p>Guideline 6-3. Incorporate safe mode for space-borne processing subsystems</p> <p>Recommendation:</p> <ul style="list-style-type: none"> • Include a simple, robust “safe-mode” capability. • Include a bootstrap function for loading full operational software, in non-volatile memory. • Design and implement safe mode to be entered after some system-dependent event(s), period of inactivity, or upon ground initiated command.
<p>Evaluation Criteria: Operator command or <system dependent> alarms or conditions will be able to restore minimal system operations via the safe mode for a failed or otherwise disabled bus or payload subsystem.</p>
<p>Milestone: System acquisition and capability updates</p>
<p>Rationale: Without on-orbit physical access an automated safe mode is necessary to recover from anomalous states that might otherwise hang the system in a non-operational state.</p>
<p>Stakeholders/Actions:</p> <ul style="list-style-type: none"> • System Operator should provide input through all design stages so that implemented capabilities can be used appropriately to achieve safe mode capability, including entry and exit from safe mode. • Program Office must assure that requirements for safe mode, and its entry conditions and exit conditions, are in place before development. • Developer must provide system capabilities meeting the requirements for safe mode entry, operation, and exit.

Guideline 6-4. Protect the safe mode from unauthorized activation

Recommendation:

- Protect the safe mode to prevent its use as a Denial-of-Service (DoS) vector: only <system dependent> alarms, executive processes or authenticated operator command(s) can trigger the safe mode.
- Enable system operator to force revert to normal mode and temporarily disable selected alarm-based transitions to safe mode.

Evaluation Criteria: External activation requires a system operator authenticated command. System dependent internal alarms trigger safe mode.

Milestone: System acquisition and capability updates

Rationale: Exploitation of safe mode by an untrusted process or invalid command could otherwise seriously degrade or prevent useful mission operations.

Stakeholders/Actions:

- System Operator should provide input through all design stages so that implemented capabilities provide appropriate operator-driven safe mode triggering, exit/reversion, and alarm disablement.
- Program Office must assure that requirements for hardened/protected safe mode entry and exit mechanisms are in place before development.
- Developer must provide system capabilities meeting the requirements for hardened/protected safe mode entry and exit mechanisms.

Guideline 6-5. Protect full and partial space segment operational software and database upload capability

Recommendation:

- Protect space-borne operational software and database updates via a cryptographically signed image and an authenticated operator command.
- As part of the update process, ensure that an operator may also rollback the most recent update via an authenticated command.

Evaluation Criteria: New operational SW becomes operational after verification and operator command, SW image with invalid signature or data corruption is dropped, update is not activated for use without operator command, and operation success or failure is indicated. Operator has ability to command a rollback for a <system dependent> time after activation.

Milestone: System acquisition and capability updates

Rationale: Secure upload verification is needed to prevent an adversary, insider or error process from subverting or corrupting system software or databases and thereby causing a mission failure. Rollback is needed in case operational system function is negatively impacted by the update.

Stakeholders/Actions:

- System Operator should provide input through all design stages so that implemented capabilities provide appropriate operator commanding for full and partial updates as well as rollback.
- Program Office must assure that requirements are in place before development for mechanisms to provide for full and partial updates of operational software and databases that must be crypto signed and authenticated operator commanded.
- Developer must provide system capabilities meeting the requirements for full and partial updates of operational software and databases.

6.2.2 System Hardening

6.2.2.1 Secure Space System Architectures

Awareness of the intended and actual security architecture is particularly vital for space systems to ensure that system security, integrity, and availability is not compromised over the life of the system. As space systems have become more complex and subject to on-orbit updates, this need now extends into operation for both the space and ground-based components of operational systems. Consequently, while being of primary importance during system concept and development stages, Guideline 6-6 through Guideline 6-8 are also reflected in the operational guidance of chapter 7.

Guideline 6-6. Document and maintain the system security architecture

Recommendation:

- Maintain security architecture views showing all external system interfaces (or interface categories), all security domains, and all internal security domain interconnections throughout the entire program lifecycle.
- Capture information or reference artifacts in the System Security Management Plan (SSMP).

Evaluation Criteria: Security architecture is updated, reviewed, and approved at all major milestones and periodically over system lifecycle. Connections and interactions shown during: development, integration, test, deployment, pre-launch checkout, launch, early orbit, operationally, and once decommissioned.

Milestone: System acquisition and capability updates

Rationale: Adversaries seek to exploit systems when they are least protected, installing malware or back-doors for exploitation during operations. By understanding the security architecture throughout the lifecycle (e.g., subsystem integration, third-party testing, satellite integration, launch preparation, launch and early orbit) risks to system security can be identified and mitigated.

Stakeholders/Actions:

- System Operator provides input through all design stages so that system use and actual operational system interfaces are well understood and reflected in the security architecture. Operator input is also used to ensure that the security architecture enables rather than precludes efficient operation.
- Program Office provides enterprise architectural context for the system under development, ensures that a complete, consistent, and correct system security architecture is maintained and involves the necessary stakeholders for architecture validation.
- Developer synthesizes the security architecture from system security requirements, system operation concepts, and system architecture, then maintains and matures security architecture throughout the development phase, providing it as a deliverable for use by the system operator after system handover.

Guideline 6-7. Policy monitoring and third-party analysis to ensure security policy compliance

Recommendation:

- Track applicable security policy for impacts to the security architecture and design.
- Provide trusted and independent third-party analysis report at major reviews to document any policy concerns among interconnected domains and security functionality gaps.

Evaluation Criteria: Analysis by AO-approved, independent third party of system security policy and functionality issues available at major reviews and periodically during operation identifies risks to system security posture.

Milestone: System acquisition and capability updates

Rationale: Evolution of information system technologies, and in the threat and regulatory environment, results in a shift in governing policy over time. Policy compliance is necessary for system Certification and Accreditation; failures to comply can result in a denial of authorization to operate.

Stakeholders/Actions:

- AO approves third party analyst selection, or recommends an alternative then reviews and approves policies to be considered in the analysis, the analysis findings and any suggested mitigations.
- In coordination with the Authorizing Official (AO) the Program Office selects, contracts for, and manages the third-party analysis effort, then coordinates with the AO and developer to determine any necessary mitigation approaches, tasking the developer to implement selected mitigations.
- Developer monitors policy activity as part of the IA Integrated Product Team (IPT), provides access to needed design and architecture documentation, works with program office and analyst to define mitigations, implements required system updates.

Guideline 6-8. Protect all space segment security boundaries, document risk and mitigate uncontrolled boundaries

Recommendation:

- Control – or at least document – the risk associated with all space segment (i.e., space, link, and ground) security boundaries based on the security domains and policies resulting from Guideline 6-6 and Guideline 6-7.
- At a minimum Medium Robustness (i.e., EAL level 3 to 4) IA and IA-enabled products are to be used for controlling security boundaries.

Evaluation Criteria: Policy monitoring and third-party analysis to ensure security policy per Guideline 6-7 results in acceptable levels of risk to compromise of system security, integrity, and availability policies, with concurrence of applicable program office management, CA, AO and/or Operational command. Security boundary controls are verified for effectiveness, which may include: trusted OS, multi-domain architecture, integrity and security domain crossing controls, control flow monitoring, HW-assisted address boundary checks, process interaction white-lists, covert channel mitigation, and segregation of critical network traffic (e.g., management or control) from user traffic.

Milestone: System acquisition and capability updates

Rationale: The legacy practice of “system-high” satellite operation was acceptable due to relative isolation of NSS-S ground elements and the satellite’s mostly analog communication elements. However, interconnections of NSS-S ground elements to diverse other ground networks coupled with the pervasive use of processors, sophisticated digital HW, and programmable controllers within “Black” satellite subsystems has rendered the system-high assumption generally invalid. Continuing with the system high assumption can expose classified subsystems (e.g., payload processor, command decoder or ground control network) to exploitation from the Black domain (e.g., satellite modem or ground system contractor network) by malware insertion into the Black domain migrating through unprotected boundaries.

Stakeholders/Actions:

- AO evaluates and approves mitigations and accepts residual risk.
- CA ensures that boundaries are adequately controlled and security measures verified to be effective.
- System Operator assists in defining necessary operational interfaces, reviews and provides input for boundary control measures and procedures.
- Program Office ensures security boundaries are identified, mitigated, and the control measures are verified and certified, as required.
- Developer documents all system security boundaries, identifies risks and mitigations to those boundaries, implements mitigations, performs and documents boundary verification testing.

6.2.2.2 Limit Vulnerability Introduction

Protection of space assets against the advanced cyber threat can leverage crypto system software and development environment integrity practices which parallel the best practices of space system SW and Firmware (FW) development per the specific recommendations of Guideline 6-9.

<p>Guideline 6-9. Ensure robust program protection for flight SW components</p> <p>Recommendation:</p> <ul style="list-style-type: none"> • Include all flight SW architecture, design, executables, and development tools in the Program Protection Plan.
<p>Evaluation Criteria: Flight SW artifacts, components, and infrastructure addressed by the PPP.</p>
<p>Milestone: System acquisition and capability updates</p>
<p>Rationale: Protection of SW artifacts from inception through decommissioning reduces the probability of successful adversarial system SW vulnerability analysis, attack formulation and malware insertion.</p>
<p>Stakeholders/Actions:</p> <ul style="list-style-type: none"> • System Operator provides inputs for determining critical SW components during operations and operational protection considerations that might impact system requirements or program protection during development. • Program Office coordinates, requires, approves and monitors protection of flight SW components, including handoff to operations. • Developer generates and implements adequate flight SW protection measures during development.

6.2.2.3 Security Analysis and Testing

As referenced in section 6.1.1, due diligence for implementing, testing, and certifying NSS-S to their applicable IA standards is assumed to ensure verification of secure configurations and functionality in space components as a part of system Integration and Testing (I&T), third-party analysis and testing of security-critical functionality and certification of space components to relevant government standards. However, mitigation of the advanced cyber threat warrants additional analysis and testing, and leveraging current intelligence estimates of adversarial capabilities and intent, as provided in Guideline 6-10.

Guideline 6-10. Provide system subversion analysis and test

Recommendation:

- Include a third-party analysis and test organization to subject the system to blue and/or red team attacks using realistic, system-specific, intelligence-driven attack scenarios
- Scenarios to consider include: malicious insider, compromised user terminal, malicious international partner, adversarial signal exploitation, external system stimulus or mission spoofing

Evaluation Criteria: Third-party subversion analysis and/or tests completed, results prioritized and mitigated as appropriate and practical.

Milestone: System acquisition and capability updates

Rationale: System designers generally have an implicit assumption that the system will be used and treated as designed; however, adversaries will exploit features in unanticipated ways to subvert or compromise the mission. This task uses the best available intelligence and “friendly” testers skilled in system exploitation to expose weaknesses, thus enabling informed risk mitigation or acceptance.

Stakeholders/Actions:

- AO approves third-party tester selection, reviews and approves test results and any needed mitigations
- System Operator provides input to attack scenarios and mitigation approaches, as applicable may provide access to a test or operational system for the testing.
- In coordination with the AO the Program Office selects, contracts for, and manages the third-party test effort, then coordinates with all stakeholders through the IA IPT to determine testing strategy and any necessary mitigation approaches, tasking the developer to implement selected mitigations.
- Developer provides access to needed documentation and operational system elements, works with program office and tester to define mitigations, and implements required system updates.

6.2.3 System Monitoring

Identification and logging of security events within the space component (e.g., SW updates, Communications Security (COMSEC)/Transmission Security (TRANSEC) status and control, security component management, other significant state changes and user/operator actions) is assumed as part of auditing requirements per normal IA standards, as is identifying data within the space component for use by Security Management Automation capability within the operating environment. But, to further harden existing and future systems against the emerging cyber threat Guideline 6-11 is also recommended.

<p>Guideline 6-11. Exploit standard telemetry streams for cyber situational awareness</p> <p>Recommendation:</p> <ul style="list-style-type: none"> • Provide all standard telemetry as input for data mining and analysis for indications of cyber attack and security events. • As applicable incorporate new cyber-specific telemetry monitors
<p>Evaluation Criteria: Standard telemetry data leveraged for cyber situational awareness, as applicable cyber-specific monitors, enables enhanced awareness based on telemetry data.</p>
<p>Milestone: System acquisition and capability updates</p>
<p>Rationale: Sophisticated pattern recognition and data mining techniques, as practiced in intrusion detection systems, and malware detection and cyber attack forensics may be leveraged to provide increased cyber situational awareness (CSA) for all NSS-S systems exploiting built-in space system telemetry reporting capability. As with any defensive operation, situational awareness is essential for mitigating attacks.</p>
<p>Stakeholders/Actions:</p> <ul style="list-style-type: none"> • System Operator provides insight into operational constraints, potential ground system resources and operational tradeoffs for use of telemetry streams for CSA. • Program Office provides system threat and vulnerability assessment data, coordinates and tasks the effort to implement usage of the system telemetry stream for CSA. • Developer coordinates with operator and program office to define effective usage of telemetry for CSA then implements the approved approach.

6.3 Cyber Hardening for the Space Segment

In addition to Addressing the Advanced Cyber Threat for NSS-Space Components as detailed in section 6.2, and NSS-S Ground Enclave Mission Assurance per section 6.1.2, it is also necessary to ensure that the space-segment, taken as a whole, implements coherent and secure development practices and system architectures. Towards that end the following best practices are recommended.

6.3.1 Enhanced Program Protection

Protection of critical program information (CPI) is already required by DODI 5200.39, and OSD is pushing for its employment more consistently across large DOD programs. This addresses, but only in part, the need for Program Protection identified in chapter 5.

As motivation for enhanced Program Protection during development, TOR-2009(1455)-6 provides the following scenario:

“During system development, personnel in government and contractor organizations exchange information over computer networks. An adversary who gains access to those information exchanges and/or to the development information systems could analyze the system design and identify possible points of attack. He could also surreptitiously insert hardware or software into the system, laying a foundation for malicious activity when the system is operational.”

An adversary will naturally seek low risk and lower cost ways to attack or otherwise compromise the effectiveness of a system, often by gaining access to and exploiting or subverting system information or components. This adversarial activity will not wait until the system is fielded with all protections in

place; rather it begins at system inception, probing for poorly protected information and continues throughout the entire lifecycle. NSS-S system design, components, contractors, subcontractors, development tools, subsystems, integration and test environments, early releases and fielded (captured) elements are all subject to exploitation and therefore need prudent protections. Particularly for high-value NSS-S system a broader-than-usual view of critical information and components needs to be identified and plans for protecting program information and components defined, see Guideline 6-12 and Guideline 6-13. These enhanced program protection measures provide the development phase guidance in response to “Establish and Implement Access Understand/Control functions” in response to Guideline 4-2. The protection needs for a program should be periodically re-evaluated as the threat environment changes, system attributes are exposed and systems are exposed via previously unanticipated forward deployments. Note that protection needs may increase or decrease as a result of this review and protection processes or technical features may be added or retired.

Guideline 6-12. Periodically identify critical program information, technology and components

Recommendation:

- Periodically assess the full range of system information, technologies and components (or in general “artifacts”) to identify those that, if compromised, could reasonably be expected to enable an adversary to compromise the intended mission.
- Identify all lifecycle touch-points for each of the identified important artifacts.
- As applicable flow protection needs into the Supply Chain Risk Management (SCRM) plan.
- Update the Program Protection Plan (PPP) in response to critical program artifact reassessments.

Evaluation Criteria: Stakeholder concurrence that important information has been identified.

Milestone: As part of solicitation response, updated at each major design review during system acquisition and capability updates

Rationale: Adversaries seek to compromise or otherwise mitigate the operational effectiveness of systems early in the program life-cycle when they are least protected. Mitigation of this threat requires that information and components be identified during initial program planning and in the solicitation response, be expanded and updated during the development process, and be maintained during operations.

Stakeholders/Actions:

- System Operator provides inputs for determining critical program information, components and systems (i.e., program artifacts) during operations.
- Program Office provides current program threat information to the developer; and coordinates, requires, and approves critical program artifact list.
- Developer works with the Program Office to identify a detailed critical program artifact list based on their specific system design, periodically updates critical program artifact list as the design matures and new threat information is provided by the program office. Coordinates and incorporates subcontractor input to the critical program artifact list.
- Subcontractors support developer in generation of critical program artifacts incorporated in their subsystem(s).

Guideline 6-13. Risk-based Program Protection and Supply Chain Risk Management Plans Recommendation:

- Generate streamlined Program Protection and Supply Chain Risk Management Plans (PPP/SCRMP) identifying all important applicable program information, technologies and components, associating with each the planned protections.
- Include: personnel training, cryptographic methods for controlling configurations during development, two-factor authentication for internet document repositories, secured internet transfer of all program information, telephone conference protection, and portable storage encryption.
- Use PPP/SCRMP to roll down necessary controls from 1st tier contractors and major subcontractors to vendors.

Evaluation Criteria: Stakeholder concurrence that important program information is adequately protected via review of developer accountability documentation PPP and SCRMP(s).

Milestone: As part of solicitation response, updated at each major design review during system acquisition and capability updates.

Rationale: Protection of key technologies, components, and information systems is necessary throughout the program lifecycle to preclude subversion of the information system and therefore its mission and mission information.

Stakeholders/Actions:

- System Operator provides inputs for determining operational protection considerations that might impact system requirements or program protection during development.
- Program Office coordinates, requires, approves, and monitors protection of critical program artifacts including handoff to operations.
- Developer generates streamlined Program Protection and Supply Chain Risk Management Plans (PPP/SCRMP); based on these plans, implements adequate critical program artifact protection measures during development, flows applicable critical artifact protection requirements to subcontractors and vendors, requires a PPP from major subcontractors; and monitors their compliance.
- Subcontractors generate and implement adequate critical program artifact protection measures, flow applicable critical artifact protection requirements to vendors, require a PPP from lower-tier subcontractors and monitor their compliance.
- Vendors generate and implement required critical program artifact protection measures.

6.3.2 Developing Mission Resilience

In addition, the needed extensions of practices and requirements developed in response to normal Information Assurance policy (e.g., ICD 503, CNSSI-1253 and NIST SP 800-53), specific development-focused measures are needed to incorporate mission resilience in response to the advance cyber threat. Guideline 6-14 through Guideline 6-19 below provide development-focused guidance for implementing system cyber resilience, with references to specific chapter 4 guidelines included in each. This section guidance assumes that the chapter 4 guidelines are completed and the associated artifacts in place, then provides recommendations for developing the associated protection measures or processes as applicable for implementation within a NSS-S system.

<p>Guideline 6-14. Architectural trades for resilient mission-information exchanges to drive Mission Risk Management Approach</p> <p>Recommendation:</p> <ul style="list-style-type: none"> • Integrate system functional requirements with the government prioritized risk management framework controls to synthesize an effective and affordable system architecture in response to Guideline 4-1: “Perform mission-driven analysis to determine mission-information dependencies.”
<p>Evaluation Criteria: Stakeholder approval of likely effectiveness, cost and user impact of mission-information exchange driven architectural impacts.</p>
<p>Milestone: Acquisition response, updated at System Design Review</p>
<p>Rationale: Mission assurance in the face of cyber attack requires integrated system infrastructure to facilitate information protection and operational courses of action according to the greatest potential impact to mission success.</p>
<p>Stakeholders/Actions:</p> <ul style="list-style-type: none"> • Program Office provides baseline Mission-Driven Assessment, mission-information dependencies, prioritized risk management framework controls and system functional requirements. • Developer: <ul style="list-style-type: none"> – Generates requirements and design approach to meet mission-based measurement and user interface requirements, documents high priority mission information risk item mitigations, and documents residual mission information risk upon system delivery. – Participates in Mission-Driven Assessment, to include assisting in Measure of Effectiveness selection, mission impact assessment, and mitigation evaluation. Incorporates the MDA results into test/evaluation planning to include test environment configuration, test scenarios, and high priority mission operations primary and secondary execution.

Guideline 6-15. Derive and implement system requirements to support operational access control

Recommendation:

- Derive detailed system requirements in support of Guideline 4-2 “Implement Access Control functions across system lifecycle.”

Evaluation Criteria: Stakeholder approval of requirements, design and effectiveness analysis of operational access control driven system requirements.

Milestone: System Requirements Review, Preliminary Design Review, Critical Design Review

Rationale: Some automation of operational access control functions will generally be necessary to effectively manage system accesses, denying unauthorized access while not unduly delaying new authorized users.

Stakeholders/Actions:

- System Operator provides input on access needs to influence system technical capabilities.
- Program Office coordinates necessary interactions with system stakeholders in support of operational access control and provides access control guidelines, process and functional requirements.
- Developer:
 - Develops and maintains Access Control approach, administers assigned Access Control management functions, accounts for Access Control management – encompassing all subcontractors, vendors, business systems, and tools.
 - Provides input on test evaluation access needs to provide early influence on system capabilities.

Guideline 6-16. Derive and implement system requirements from system resilience architecture and trust profiles

Recommendation:

- Derive detailed system trust requirements from the trust profiles generated per Guideline 4-3 “Develop measurement plan and associated instrumentation approach” and the resilient architecture resulting from Guideline 6-14.

Evaluation Criteria: Stakeholder approval of requirements, design, and effectiveness analysis of system resilience and trust profile driven system requirements. Instrumented feeds from the cyber environment clearly provides required measurements and are clearly traceable through aggregation to association with potential impacts to mission outcome.

Milestone: System Requirements Review, Preliminary Design Review, Critical Design Review

Rationale: Implementation of detailed system requirements assures that a trusted computing environment is available to support good integrity in the measurements of cyber state and the subsequent calculation of potential impact to mission outcome for robust cyber mission assurance (CMA).

Stakeholders/Actions:

- System Operator provides input to measurement and instrumentation requirements and trust profiles.
- Program Office provides trust profiles, requirements and program plan.
- Developer generates detailed system trust requirements, design and system instrumentation approach, test facilities and test cases to verify the required measurement and trust profile capabilities.

Guideline 6-17. Derive and implement IA component cyber event instrumentation requirements

Recommendation:

- Refine and update government furnished Mission-Driven information risk assessment
- Generate component requirements to provide instrumentation feeds from the appropriate IA system components.
- Implement the program cyber measurement plan developed per Guideline 4-3, “Develop measurement plan and associated instrumentation approach” and Guideline 4-1 “Perform mission-driven analysis to determine mission-information dependencies.”
- Implement cyber instrumentation requirements and document unaddressed mission information risk areas.

Evaluation Criteria: Stakeholder approval of requirements, design, effectiveness analysis of cyber event instrumentation requirements, all required cyber measurement information data is incorporated in the telemetry stream (directly for necessary high-level measurands and may be multiplexed into the telemetry stream via command for lower-level information).

Milestone: Concept as part of solicitation response, requirements, analysis, design and remaining risk updated at each major design review (i.e., System through Final Design reviews).

Rationale: Provide the cyber feed requirements to enable cyber situational awareness in support of operational course of action decision support, but recognizing that telemetry bandwidth is generally constrained allows for normally non-essential information to only be provided upon request.

Stakeholders/Actions:

- Program Office validates trust profiles, cyber instrumentation approach and developers trust profile documentation and maintenance program plan.
- Developer implements system trust-profile based requirements, cyber instrumentation approach, verifies the required trust profile and measurement capabilities, documenting trust profiles per plan.
- IA component vendors provide and/or configure IA components to meet design measurement approach.

Guideline 6-18. Provide Mission-based Cyber Situational Awareness display

Recommendation:

- Generate detailed display synthesis and display requirements for effective user awareness of the dynamic system cyber situation in support of Guideline 4-4 “Require Mission-based Cyber Situational Awareness.”
- CSA displays will leverage measurement profiles already calculated and display CSA in terms of potential impact to mission success.

Evaluation Criteria: Stakeholder approval of CSA display concept, requirements, design, and usefulness to system operator.

Milestone: Concept as part of solicitation response, detailed display operational concepts, usability, design and effectiveness updated at each major design review.

Rationale: Cyber mission assurance requires that the operators (spacecraft, system, and mission owners) are provided cyber status in a format that permits determination of potential impact to mission outcome and to plan appropriate courses of action.

Stakeholders/Actions:

- System Operator provides input to the development process regarding CSA needs and operational environment.
- Program Office coordinates with the operational community to define CSA functional requirements, validates developer decomposition of functional requirements and test results.
- Developer generates, implements, and verifies CSA functional requirements with input from Operators and Program office to ensure CSA displays are effective for the system operators and users.

Guideline 6-19. Derive technical requirements in support of Cyber Course of Action

Recommendation:

- Generate and implement system functional requirements in support of Guideline 4-5 “Require Mission-based Cyber Course of Action Development.”

Evaluation Criteria: Stakeholder approval of CCOA related functional requirements, design, technical effectiveness and usefulness to system operator.

Milestone: Concept at part of solicitation response, detailed operational concepts, usability, design and effectiveness updated at each major design review.

Rationale: Cyber mission assurance requires that operational decisions regarding the cyber infrastructure are made in the context of potential impact to mission outcome. The potential speed and scale of cyber impact due to attack likely requires automated support for preplanned courses of action and flexibility for extensions based on evolving response measures and real-time operational conditions.

Stakeholders/Actions:

- System Operator provides operational environment and user constraints and needs in support of the Cyber COA management and needs for operational Tactics, Training, and Procedures (TTPs).
- Program Office coordinates with intelligence and operational communities to provide threat and operational requirements for the Cyber COA management, validate functional requirements and test results.
- Developer:
 - Coordinates with program office and system operator to generate functional requirements, design, implementation, and test in support of Cyber COA management.
 - Contributes to TTPs that align with Cyber COA management technical capabilities, specifically regarding expected system performance.

6.3.3 Program Architecture

Recognizing that National Security Space Systems are migrating away from isolated enclaves with circuit connections to enterprise-wide, shared packet services, it is increasingly necessary to include network management and cross-domain protections in the NSS-S ground and satellite elements. This need is further exacerbated by satellites providing services to multiple user communities and interconnections with heritage or future fragmented constellations. Consequently, the overall network architecture must be clearly understood with appropriate domain isolation and vulnerability mitigations as recommended in Guideline 6-20.

Guideline 6-20. Protect the NSS-S Network in its entirety**Recommendation:**

- For network architecture purposes treat the satellite and ground enclave components as network nodes.
- Monitor and protect the entire network appropriately to avoid weak links.
- Mechanisms to apply include:
 - (1) out of band network control/management,
 - (2) network attack sensors and response mechanisms,
 - (3) coherent network defense,
 - (4) safe operating modes for when the network or management functions are under attack
 - (5) and contingency operating plans.

Evaluation Criteria: Network architecture, protections and threats reviewed and residual risk accepted by procurement manager and AO as appropriate for the development or upgrade phase.

Milestone: At each major design review during system acquisition and capability updates

Rationale: Increased drive to rapidly share information across organizational and even national boundaries causes more complex interconnections and increased exposure of every asset on the network. Since adversaries will tend to exploit the weakest link in the network it is necessary to protect all network elements.

Stakeholders/Actions:

- AO reviews results of network protection certification testing and the residual risk, levying any needed mitigations and if acceptable provides an Approval to Operate (ATO) decision.
- System Operator provides input to the developer regarding necessary operational interfaces, expected evolution and operational needs in the context of the network protection mechanism designs.
- Program Office coordinates necessary stakeholders involvement in network protection via the IA IPT, provides loss of security impact categorization for major system elements, validates functional protection requirements and test results.
- Developer participates in the IA IPT to ensure effective network protection requirements are generated, implemented and verified in the context of the full system environment, and through all stages of integration, test and deployment.

6.3.4 Program Software Development

By definition system software is the domain and target of cyber attacks. Consequently special attention is needed for development of software for high-value NSS-S systems. The solid foundation of a mature and well defined SW development process (e.g., CMMI level 3 or higher) is assumed and the additional practices of Guideline 6-21 are recommended for all NSS-S. An increasingly common vector for exposure of mission critical information to the advanced cyber threat is the movement toward COTS and Free Open Source SW (FOSS). System use of COTS/FOSS can be mitigated with a small custom SW “wrapper”, allowing the economic benefit of substantial COTS/FOSS capability, while mitigating the inherent risks of subverted COTS/FOSS products. For any instance where mission critical information must be isolated from advanced cyber threats, the additional protections of objective Guideline 6-22 are recommended. This guideline leverages additional requirements commonly applied to NSA Type 1 encryptors for high assurance protection of classified information from exposure to determined national adversaries. These additional requirements are contained in the

classified NSA Information Assurance Security Requirements Document (IASRD) which is structured to allow tailoring to a specific application. Application of the IASRD to non-cryptographic systems can incorporate a wealth of IASRD process and technical requirements that are not specific to cryptographic processes and algorithms.

<p>Guideline 6-21. Implement robust SW and development processes</p> <p>Recommendation: Implement robust SW and development processes, with the following properties:</p> <ul style="list-style-type: none"> • Cyber mission assurance information dependency and system security goals are reflected in SW architecture, design, and procurement. • COTS/FOSS capabilities are isolated, using for example, software wrappers. • Static analysis tools verify secure coding practices. • Test analysis confirms that all SW fragments are either exercised and verified during test, or those not exercised are evaluated explicitly for risk. • In association with Change Control Management, a cryptographic integrity mechanism (e.g., digital signature) ensures no unauthorized changes from the verified baseline. • Supply chain risk management applies for all SW procurements. • SW developers are all U.S. citizens.
<p>Evaluation Criteria: SW architecture, design, documentation and process verified to meet security goals. Verification that: information critical to mission success is protected in accordance with its value and threat. Storage and transport of SW source and executable code is protected with, at a minimum, FIPS 140-2 Level 1 approved cryptographic integrity mechanism(s). Developers of custom SW confirmed U.S. citizens.</p>
<p>Milestone: All SW design reviews during system acquisition and capability updates.</p>
<p>Rationale: A robust SW security architecture and development process significantly reduces the risk of system subversion. Secure coding practices and testing all paths precludes unintended functionality insertion, U.S. citizens are less likely to be influenced by foreign adversaries to subvert the system.</p>
<p>Stakeholders/Actions:</p> <ul style="list-style-type: none"> • Program Office requires a mature SW process (e.g., CMMI level 3 or higher) as a prequalification for developers. Reviews documentation, process, and SW product to ensure robust practices are followed. • Developer (and SW subcontractors) provides documentation of SW development process, implements robust practices and monitors process, documentation and SW product via an independent internal SW Quality Assurance function. Requires and monitors similar processes and documentation from SW subcontractors. Ensure that vendor-supplied SW is developed in accordance with program constraints (e.g., no foreign control, anonymity of application or customer).

Guideline 6-22. Implement enhanced SW robustness for mission critical information objects per the NSA IASRD (OBJ)

Recommendation:

- Software implementations of critical importance to the system mission assurance posture implement applicable requirements, process, and documentation from the NSA IASRD.
- Employ cleared developers and perform development in a classified or otherwise isolated environment for SW implementation needing enhanced robustness.
- Trusted software providers for all enhanced SW robustness procurements.

Evaluation Criteria: Independent review and validation of development process, system design and documentation to the selected IASRD requirements.

Milestone: All SW design reviews during system acquisition and capability updates

Rationale: Enhanced SW robustness is needed to protect mission critical information from the advanced threat and can leverage the well-established practices, as documented in the NSA IASRD for Type 1 encryptors, which must protect classified information from determined national adversaries.

Stakeholders/Actions:

- Program Office coordinates with NSA to provide a tailored IASRD, providing only the requirements appropriate to the application. Monitors and reviews process and documentation to ensure enhanced SW robustness practices and products.
- Developer (and SW subcontractors) incorporates applicable IASRD requirements into development processes impacting mission critical information, implements applicable IASRD required functions, documents, and reviews per the robust practices of Guideline 6-22. Requires and monitors similar processes and documentation from SW subcontractors, ensures that vendor supplied SW meets IASRD requirements.

6.3.5 Program Hardware Development

The use of Hardware Description Languages (HDLs), Intellectual Property (IP) cores, Field Programmable Gate Arrays (FPGAs), and Integrated Circuits (IC) technologies supporting over 100 million gates have enabled the complexity and functionality of HW systems and components to be on par with that of SW systems. Space systems are increasingly leveraging these capabilities and because of the parallels with SW systems (e.g., HDL \approx SW, IP cores \approx COTS SW libraries, COTS HW synthesis tools \approx COTS SW compilers, FPGA updates \approx SW configuration updates, millions of Gates \approx millions Source Lines of Code (SLOC)) share many of the vulnerabilities to cyber-attack, particularly during development. As for SW development, a mature and well defined HW development process (i.e., CMMI level 3 or higher) is assumed and the additional practices of Guideline 6-23 are recommended for all NSS-S. As with SW systems, the increased use of COTS IP cores, FPGAs and advanced processors there is a very real risk of subverted functionality being incorporated into NSS-S system HW. For this reason a HW isolation layer may be indicated to isolate the system from such threats to mission critical information. For COTS mitigation or other scenarios where HW isolation from the advanced cyber threat is needed, the additional protections of Guideline 6-24 are also recommended. As explained in section 6.3.4 above for SW development, the IASRD also provides a wealth of applicable process and technical requirements that are not specific to cryptographic HW (including FPGA) development.

Guideline 6-23. Implement robust hardware and computing platforms

Recommendation: Implement robust hardware and computing platforms, with the following properties:

- System HW architecture, design, and procurement supports cyber mission assurance information dependency and system security goals.
- Hardware isolation later for isolation of COTS IP cores.
- Static tools verify secure firmware coding practices.
- Test analysis confirms that all HW subcomponents are either verified during test or those not exercised are evaluated for risk.
- In association with Change Control Management a cryptographic integrity mechanism (e.g., digital signature) ensures no unauthorized changes from the verified design.
- Supply chain risk management applied for all HW procurements.
- Trusted Foundries³⁴ used as available.
- HW developers are all U.S. citizens.

Evaluation Criteria: Verification that HW architecture, design, documentation, and process meet security goals; information critical to mission success is protected in accordance with its value and threat. Storage and transport of HW source and implementation data is protected with, at a minimum, FIPS 140-2 Level 1 approved cryptographic integrity mechanism(s). HW developers confirmed as U.S. citizens

Milestone: All HW/FPGA design reviews during system acquisition and capability updates

Rationale: Security design and analysis guidelines ensure a low probability of HW fault or subversion compromising system security; U.S. citizens are less likely to be subverted by foreign adversaries.

Stakeholders/Actions:

- Program Office requires a mature HW process (e.g., CMMI level 3 or higher) as a prequalification for developers. Reviews design process, design documentation, test procedures, manufacturing process and test results to ensure that robust practices are followed.
- Developer (and HW subcontractors) provides documentation of development, manufacturing and test processes, implements robust practices; monitors process, documentation, design product, test results and manufactured product via an independent internal Quality Assurance function. Requires and monitors similar processes and documentation from HW subcontractors. Ensures that vendor-supplied components are produced in accordance with program constraints (e.g., no counterfeit parts, anonymity of application or customer)

³⁴ Current list of trusted foundries with contact information is at: <http://www.dmea.osd.mil/trustedic.html>

Guideline 6-24. Implement enhanced HW assurance for protection of mission critical information per the NSA IASRD (OBJ)

Recommendation:

- Hardware implementations of critical importance to the system mission assurance posture implement applicable NSA IASRD hardware architecture and design requirements, failure analysis, and documentation requirements.
- Employ cleared developers and perform development in a classified or otherwise isolated environment for implementation of elements requiring enhanced HW assurance. Trusted Foundries used for all enhanced assurance HW procurements.

Evaluation Criteria: Validation of HW architecture, design standards, documentation, and process to the selected IASRD requirements by an independent test group. Confirmation of cleared developers and isolated development environment.

Milestone: All HW/FPGA design reviews during system acquisition and capability updates

Rationale: Enhanced HW/FPGA robustness is needed to protect mission critical information from advanced cyber threats. Incorporation of enhanced HW assurance can leverage the well-established practices documented in the NSA IASRD for Type 1 encryptors (which must protect classified information from determined national adversaries).

Stakeholders/Actions:

- Program Office coordinates with NSA to provide a tailored IASRD, providing only the requirements appropriate to the application. Monitors and reviews process and documentation to ensure enhanced HW robustness practices and products.
- Developer (and SW subcontractors) incorporates applicable IASRD requirements into development processes impacting mission critical information, implement applicable IASRD required functions, document and review per the robust practices of Guideline 6-23. Requires and monitors similar processes and documentation from HW subcontractors, ensure that vendor supplied HW meets IASRD requirements.

6.4 Prioritizing Development Activities with Constrained Resources

Given the convergence of the modern military and intelligence communities increased dependence on networked communications and the ever escalating threat environment, it is clear that cyber-security is essential. However, perfect security is unattainable and even the intended practical development guidance of this section may be beyond the resources of many programs and products. Therefore a unique balance between affordability and the recommended cyber-security measures will need to be determined for each use of this guidance document, as described in Guideline 6-25.

Guideline 6-25. Incorporate Cyber-Security approach into the System Security Management Plan

Recommendation:

- Leverage best available intelligence for system threat assessment, categories, and impacts of system information, technology availabilities, and system architecture and program resources to prioritize system cyber-security measures.
- Estimate and document the residual risk and any necessary mitigation.
- Capture approach and reference artifacts for all “Space Segment Information Assurance Guidance for Mission Success” guidelines in the SSMP.

Evaluation Criteria: Cyber-security approach is reviewed and approved by system stakeholders including procurement manager and CA/AO as applicable.

Milestone: All major design reviews during system acquisition and capability updates

Rationale: Mission assurance in a contested environment can only be provided if realistic risks are understood and mitigated to ensure that the minimum necessary system functionality is available when needed.

Stakeholders/Actions:

- AO reviews cyber-security approach, residual risk estimates and risk mitigations. Recommends needed updates and approves when a satisfactory approach and mitigations are achieved.
- CA assists in evaluation of cyber-security approach, verification methodology, residual risk estimation and determination of mitigation approaches.
- Program Office provides intelligence and threat assessment information to the program, coordinates needed stakeholder input to the Cyber-security approach through the IA IPT, facilitates needed AO and CA involvement and approvals; requires, reviews and approves cyber-security approach as part of the SSMP.
- Developer in response to the guidance of this section (i.e., Guideline 6-1 through Guideline 6-24), generates a Cyber-Security approach briefly outlining the applicability, compliance approach, or rationale for non-compliance for each guideline. Participates in the IA IPT as a principle stakeholder for refining, updating, and obtaining approval of the Cyber-Security approach. Reviews and statuses progress to the Cyber-Security plan as part of each major review. Obtains needed input from major subcontractors for the Cyber-Security approach and its implementation.
- Subcontractors participate as required in response to developer needs for the cyber-security effort.

7. National Space Segment Operations Guidance

This chapter addresses the Cyber challenges that face operators and users of space systems, specifically focusing on the steps that will improve the Space Segment information security and mission survivability and resilience. Both new systems and heritage/legacy systems will be considered.

As described in Section 1.1.5, the key behaviors that distinguish the highly resilient organizations are a culture and behavior that negate these effects, instituting a continual practice that:

1. Tracks and addresses small failures
2. Resists oversimplification that hides failures and vulnerabilities
3. Remains sensitive to the actual operational situation
4. Maintains capabilities for and commitment to resilience
5. Takes advantage of the expertise where it exists and applies that expertise where needed³⁵

These are the principles of resilient behavior that underlie the guidance provided in this chapter.

Section 7.1 focuses on specific guidance for systems that are in the sustainment phase of their existence from an acquisition point of view. Their space vehicle and payload configuration is not likely to be significantly altered in upcoming improvement cycles, because sustainment funding is not likely to cover major new developments on the space platform. And the operational considerations that will impact the resilience of functions on the space platform are primarily controlled from the ground; so this section focuses primarily on the ground control functions.

7.1 Improving space system space segment operations

Analysis of problems in existing space systems indicates that there are a set of common problem areas that emerge during operations that can be addressed with specific operations and sustainment actions. Among the most important, easily understood, and affordably addressable of these problem areas are:

- Interface and Connectivity Identification, Documentation, and Enforcement (See Section 7.1.1)
- Configuration Management/Control of Space IT Assets (See Section 7.1.2)
- Authentication and Access Management/Administration (See Section 7.1.3)
- Consistent Enforceable Standards for Sustainment/Operational System Administration (See Section 7.1.4)
- Intrusion Detection, Audit, Prevention, and Eradication (See Section 7.1.5)
- Space Segment Change Management (See Section 7.1.6)

To achieve operational/mission resilience in the presence of a dynamically changing environment of active Space Cyber threats, it is important to establish and maintain an up-to-date operational understanding of the evolving Space Cyber threats/threat vectors, and the mitigation options available with existing functions in space and in ground control capabilities (see Section 7.1.7 Changing Threat, Vulnerability and Mitigation Profiles).

³⁵ Weick and Sutcliffe, *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*, 2nd Edition, Jossey Bass, 2007.

In addition, to the extent existing system capabilities permit, it is critical to keep continuous awareness of the actual Cyber situation. See Section 7.1.8 Cyber Situation Awareness.

Finally, as new recapitalization points arise, it is important to identify affordable changes to Space Segment capabilities that enable new, more effective Cyber situation awareness and threat mitigations / attack identification and response; and to implement the most mission critical of those changes. See Section 7.1.9 Cyber Response Capability Enhancement.

7.1.1 Interface and Connectivity Identification, Documentation, and Enforcement

Awareness of the day-to-day operational security architecture is particularly critical for space systems to ensure that system security, integrity, and availability is not compromised over the life of the system. Unfortunately, it is not uncommon for basic system connectivity to external systems and users to vary over the system life-cycle, often drifting from the original operational concept, and from the assumptions that governed the design of the system. It may become altogether unclear exactly what parts of the system are connected to what other systems and users. Upon inspection, it may be discovered that there is ground control system connectivity to systems, networks, and communities that are nowhere described in operational architecture diagrams and documents, the TTPs, or any other process/system documentation. It is essential to periodically re-establish understanding of the operational security architecture (as opposed to the designed, developed, or assumed architecture), to re-assess its implications for information protection and mission resiliency, and to enforce trust properties across interfaces with other systems.

Often changes in system interfaces with other systems have a dramatic impact on the system's cyber "attack surface", admitting the most common methods for malicious cyber exploitation. When possible, it is appropriate to develop and use continuous monitoring capabilities that track/map the connectivities of the system architecture as the system is functioning. It is necessary to know at all times where the interfaces are; where they go; classification level and accreditation status of the interfacing system; ports, protocols, and services that represent "normal" behavior across the interface; or points of contact for the system on the other side of the interface.

Guideline 7-1 uses the results of, and carries forward into operations, chapter 6 recommendations captured in Guideline 6-6, Guideline 6-7, and Guideline 6-8.

Guideline 7-1. Document, maintain, and enforce the system security architecture over the system's operational lifetime

Recommendation:

- Adopt (if they exist as per Guideline 6-6) or develop (if they don't) security architecture views showing all external system interfaces, all security domains and internal security domain interconnections.
- Establish key properties of the interfacing systems and users.
- Conduct periodic third party analyses to identify all components and interfaces actually part of the operational system architecture and to ensure security policy compliance.

Evaluation Criteria: System security architecture updated, reviewed, and approved periodically during operations. Connections and interactions shown during: launch, early orbit, operationally, and once decommissioned. Interfaces that introduce excessive risk are disabled until risk can be mitigated.

Milestone: Capability insertions, operations, and sustainment

Rationale: A thorough understanding of the actual security architecture, interconnections and controls throughout the system lifecycle is necessary to achieve mission assurance in a contested Cyberspace environment. Evolution of information systems, governing policy, and threat environment necessitate a periodic evaluation of system security posture to identify and appropriately mitigate risks. To be effective this activity needs to not only happen at certification but throughout the program lifecycle.

The principle potential cyber consequences of failures in this area include:

- Failure to properly identify, quantify, and qualify external interfaces to external systems means that the AO is unable to properly assess the risk to the operational mission.
- For systems that process classified information, this means that neither the overseeing organization nor the mission operator is able to ensure the confidentiality of mission data.
- Additionally, mission owners on either side of the interface may lack situational awareness as to whether or not they are under cyber attack.
- Mission assurance in the form of information integrity and system availability is not guaranteed in an environment where the interfaces to a system are not understood, documented, and protected.

Stakeholders/Actions:

- AO: approve a qualified independent third party to determine actual operational architecture (components and interfaces) and degree of compliance with security policy.
- System operator: have a qualified, AO approved, independent third party conduct a "100% discovery scan" of each affected system to identify known, suspected, and undocumented components and interfaces; ensure security policy compliance.
- System operator: identify mission and Program Office owners for each identified interface. If owner cannot be identified, or security policy cannot be verified for that interface, terminate interface until a cognizant party is identified, documented, and validated against the security policy.
- System operator: establish and maintain Memoranda of Agreements (MOAs) between the system's overseeing AO and interfacing systems' OAs. Identify mechanisms for exchanging threat and vulnerability information; data exchange requirements; cyber event notification and management; points of contact for program management, operations, systems administration, and certification/accreditation activities; status and presence of controlled interfaces or cross domain solutions; and changes to C&A status. Ensure that these mechanisms are employed continually.
- Overseeing organization: establish and maintain a central classified database of systems and interfaces under configuration control. Require programs to regularly verify and update database.

7.1.2 Configuration Management/Control of Space IT Assets

IT assets, especially security boundary enforcement mechanisms in space systems need not only be present (the result of efforts discussed in Guideline 6-2), they also must be properly configured to perform their protective functions. Sometimes from the onset of operations, but nearly always somewhere along the path, configurations become corrupted.

Procedures to control configurations are essential; they must include periodic audits of actual configurations, and whether they are what is actually required for proper operations. Furthermore, experience often leads to changes of configurations in order to adapt to changes in the operational situation. Configuration management includes diligent tracking of those changes so that periodic audits and ongoing procedures reflect the latest ground truth operational configuration requirements. Ideally, this tracking can be accomplished continuously, with automated support. If that is programmatically feasible (e.g., if Guideline 6-2 has been followed during the development of the system so as to provide the means), continuous monitoring should be employed, along with procedures for immediately correcting discrepancies as they are discovered.

Guideline 7-2. Develop and maintain a comprehensive System Configuration Management process
Recommendation: Document, maintain, and regularly audit the system configuration.
Evaluation Criteria: Reviews determine whether procedures are in place and are performed with sufficient frequency to provide an adequate assessment of operational risk. Automated means for auditing/monitoring are employed when available.
Milestone: Throughout operations and sustainment.
Rationale: The principle potential cyber consequences of failures in this area include: <ul style="list-style-type: none">• Unacknowledged expansion of the cyber attack surface of the system, putting the system (and the mission) at potentially greater risk of being compromised than is understood• Reduced ability to ascertain whether the system is actually under cyber attack.• Severely reduced ability to establish a rapid recovery from the effects of cyber attack.
Stakeholders/Actions: <ul style="list-style-type: none">• System operator: document the system configuration. Apply applicable STIGs. Document device configurations to include all settings; serial and model numbers; locations; passwords; authorized users; ports, protocols, and services allowed; restoration priorities; software versions and patch levels; and points of contact associated with the system.• System operator: maintain the system configuration. Identify mechanisms (including continuous automated monitoring capabilities if they are available) for auditing access to privileged functions and key events. Identify incident management response actions associated with the device.• System operator: periodically audit the system configuration. Re-establish a valid map of the actual architecture of the system, its interfaces to the external world, its internal connectivities, and all the IA enabled and IT devices on the system. Determine the current configurations of the system including the IA/IT devices.• Overseeing organization: check auditing function for timeliness, completeness, and validity.

7.1.3 Authentication and Access Management/Administration

Weak or poorly protected authentication methods, upon which access control is based, have been the historic first point of attack for all levels of cyber adversary. The most common method, the use of passwords, is a weak method of authentication from the outset, and it is rendered even weaker by

procedural practices that fail to protect the passwords. While technical capabilities enable password-based (and other authentication means-based) security, they must be supported through use of procedural security mechanisms. Failure to do so impacts confidentiality, integrity, and availability of systems. In some instances, non-compliant passwords associated with antiquated applications software and system components (for example) may not be brought into compliance. Upon discovery, non-compliant password-based (or other authentication means-based) boundary protection or IA enabled devices must be corrected on the spot. Some systems are designed to employ multiple means of authentication, usually including some type of password mechanism; while these can be intrinsically more effective than those that rely on a single means of authentication, they, too, remain vulnerable to poor operational practices.

The following guideline depends upon development of access control capabilities as recommended in Guideline 6-15.

<p>Guideline 7-3. Verify and maintain authentication compliance for fielded systems</p> <p>Recommendation:</p> <ul style="list-style-type: none"> • For all authentication methods used to control access within the system, establish, publish, train and enforce system policies for their protection and use on core system components, core and boundary network devices, as well as all other relevant system components, commensurate with known or predicted threats. Start with password policies, but include all authentication mechanisms. • Conduct audits of passwords and other authentication methods and promptly correct non-compliance with applicable policies.
<p>Evaluation Criteria: Certification and accreditation (C&A) reviews determine whether procedures are in place and are performed with sufficient frequency to provide an adequate assessment of operational risk.</p>
<p>Milestone: Throughout operations and sustainment.</p>
<p>Rationale: The principle potential cyber consequences of failures in this area include:</p> <ul style="list-style-type: none"> • Weak, missing, or poorly administered authentication methods (e.g., and especially: passwords) on core system components, network components, and accounts with privileged access degrade system confidentiality, integrity, and availability. • It is highly probable that precedent already exists within the security community regarding the intentional or negligent configuration or misconfiguration of a system in such a fashion that it discloses classified or sensitive data or makes classified or sensitive data available to those without a need-to-know.
<p>Stakeholders/Actions:</p> <ul style="list-style-type: none"> • Program Office/System operator Unit: Conduct 100% audit of fielded systems to include network devices to determine whether they are conforming to appropriate agency defined policies for management of authentication information (e.g., passwords). • Overseeing organization: Ensure authentication standards are published as a standard and mandated for prime, sub-contractor, and sustainment contractor performance. • Program Office: Define contractual terms with significant monetary and/or administrative penalties for failure to implement and enforce authentication protections. • FFRDC/National Security organization: Examine options for implementation of PKI enabled or other multi-factor/robust authentication technology. Where feasible, work with the other stakeholders to introduce them in the development requirements and operational policies for new systems and systems to undergo upgrade/recapitalization.

7.1.4 Consistent Enforceable Standards for Sustainment/Operational System Administration

Consistent, enforceable standards are often not incorporated into sustainment contracts.

<p>Guideline 7-4. Develop and maintain enforceable standards for administration of fielded systems</p> <p>Recommendation:</p> <ul style="list-style-type: none"> Establish enforceable standards for system administration qualifications, requirements, and operational procedures and enforce those standards.
<p>Evaluation Criteria: Contractual reviews ensure that system administration qualifications, requirements, and operational procedures are in accordance with enforceable standards.</p>
<p>Milestone: Throughout operations and sustainment.</p>
<p>Rationale: The principle potential cyber consequences of failures in this area include:</p> <ul style="list-style-type: none"> System administrators frequently do not meet information assurance training and certification requirements (e.g., DODD 8570.1) or appropriate agency security investigation requirements. Systems are inconsistently administered; in some cases, technical security features are bypassed for convenience; and operational user manuals, when available, are not followed. Inconsistent operation of fielded systems circumvents IA design features and procedural mitigations leaving them open to confidentiality, integrity, and availability risks.
<p>Stakeholders/Actions:</p> <ul style="list-style-type: none"> Program Office: Conduct review of and document current IA sustainment/operational support contract requirements, performance, and qualifications. Overseeing Organization: Develop and publish clear, consistent, enforceable standards for IA and system administration for sustainment and operational support of its systems. Overseeing Organization: Establish standard base-lined job descriptions for IA and system administrator positions to be incorporated into sustainment and operations support contracts. Overseeing Organization: Develop standardized contractual language for use in requests for proposal.

7.1.5 Intrusion Detection, Audit, Prevention, and Eradication

Many systems consistently lack intrusion detection, prevention, eradication, and auditing.

Note that there is currently a lack of intrusion detection capabilities that are space-qualified and/or designed for use with real-time/embedded systems. In practical terms, until such capabilities are available, this guideline is applicable only to the ground control functions within the scope of “Space Segment” as defined in Section 1.1.3.

The following guideline depends upon analyses and development-produced mechanisms as recommended in Guideline 6-20.

Guideline 7-5. Implement appropriate intrusion detection and audit capabilities.

Recommendation:

- Apply intrusion-event detection services throughout the system’s operational lifetime.
- Institute auditing of intrusion events to understand system performance past and current; use that understanding to institute procedures, and identify future technical upgrades, that will result in intrusion prevention, and where possible, eradication.

Evaluation Criteria: Certification and accreditation (C&A) reviews determine whether procedures are in place and are performed with sufficient frequency to provide an adequate assessment of operational risk.

Milestone: Throughout operations and sustainment.

Rationale: The principal potential cyber consequences of failures in this area include:

- The ability to detect intrusions in networks and systems is a precursor to the ability to operate through a cyber event.
- All aspects of information and mission assurance are jeopardized by (1) inability to detect intrusions, coupled with (2) failure to conduct an independent activity to audit events to understand past and current system performance, for purposes of intrusion prevention and eradication.

Stakeholders/Actions:

- FFRDC/System operator: Examine NSS-wide common solutions for host-based and network-based intrusion systems and their general applicability to developed space systems, as well as auditing procedures and technologies leading to the development of methods for intrusion prevention and eradication.
- FFRDC/ System operator: Where necessary or beneficial, develop revised CONOPS, and identify technical capability alternatives. Consider integration with mission command operations with NSA’s Threat Operations Centers as possible options.
- FFRDC/Overseeing Organization: Investigate potential to employ appropriate agency Network Operating System Centers (NOSC) to provide intrusion detection services for space mission systems.

7.1.6 Space Segment Change Management

Systems frequently lack an effective mechanism to monitor, assess, and apply operating and application system patches. To use a DOD example, they are unable to respond to Joint Task Force for Global Network Operations (JTF-GNO) Time Compliance Network Orders (TCNOs) directing actions to protect space system networks. The following guideline depends upon development of capabilities for low-level patching of the space segment.

Guideline 7-6. Implement patch management plan.

Recommendation:

- Develop a patch management plan to ensure security patches to space segment assets and required protection requirements are maintained and up-to-date. To the extent possible, define the following to minimize introduction of unanticipated adverse risks to system operation:
 - System-dependent safe-guards for safe-mode memory updates
 - Thorough pre-patch-execution evaluation and test
 - Authenticated commands
 - Approval from operational command
- Implement the plan.

Evaluation Criteria: For systems developed under DIACAP, Certification and accreditation (C&A) reviews determine whether procedures are in place and are performed with sufficient frequency to provide an adequate assessment of operational risk. Analogous criteria apply to systems under other control regimes (e.g., NIST Risk Management Framework).

Milestone: Throughout operations and sustainment.

Rationale: Low-level patching may be required as a contingency if the primary update process fails or would unduly disrupt critical mission operations; however, due to the inherent risks the process must be carefully controlled since it overrides normal safeguards and can do irreparable damage.

The principal potential cyber consequences of failures in this area include:

Cyber defense posture of fielded systems will lag cyber threats by several months and/or years, as is often the case currently.

Stakeholders/Actions:

- Overseeing Organization/Program Office: Identify and document current strategy and processes for patch (and, for example, TCNO management) for each affected system.
- FFRDC/Overseeing Organization/Program Office: Conduct architectural assessment of systems to determine whether patch (and, for example, TCNO management) can be tailored to specific architectural designs of systems thereby increasing protection while simultaneously decreasing programmatic risk.
- Overseeing Organization/Program Office/AO: Examine centralized organization process for tracking impacts and implementation of patch (and, for example, TCNO management) activities for agency resourced space systems.

7.1.7 Changing Threat, Vulnerability and Mitigation Profiles

The Space Cyber threat environment is changing continually, and the operational environment may also be changing as described above. Consequently, both vulnerabilities and mitigations may be changing as well. Vulnerabilities in flux may include known vulnerabilities whose potential mission impact has changed over time, as well as latent as-yet unidentified (“zero day”) vulnerabilities. Mitigations may be limited by the capabilities in place both on the space vehicle itself and on the ground control system.

<p>Guideline 7-7. Conduct periodic threat, vulnerability, and mitigation reassessments</p> <p>Recommendation:</p> <ul style="list-style-type: none"> Periodically conduct vulnerability/mitigation analyses based on updated threat profiles.
<p>Evaluation Criteria: Threat, vulnerability, and mitigation assessments determine whether procedures in place address current threat environment to provide an adequate assessment of operational risk.</p>
<p>Milestone: Throughout operations and sustainment, as often as is affordable, and at least once before each recapitalization cycle.</p>
<p>Rationale: Necessary to understand the evolving nature of viable threats against continued mission effectiveness. Essential to enable the development and establishment of new operational procedures that contribute to maintaining mission-critical information confidentiality, integrity, and availability, and to identify system upgrade options that can enable additional improvements in mission resilience. The principal potential cyber consequences of failure to identify changes in threat, vulnerability, and mitigation possibilities include that adversaries may discover new ways to defeat system capabilities and subvert mission operations by limiting/preventing the ability to “fight/operate through” Space Cyber attacks.</p>
<p>Stakeholders/Actions:</p> <ul style="list-style-type: none"> Overseeing Organization/Program Office: Prioritize, determine a schedule, and commit to funding for conducting periodic reassessments of threat, vulnerability, and mitigation profiles for mission-critical systems. Overseeing Organization/Program Office: Have a qualified, AO approved, independent third party conduct the reassessments according to the prioritized schedule. AO/Overseeing Organization/Program Office: Establish a threshold of risk that is acceptable and that which is not. Fund the mitigation actions for those that address unacceptable risk.

7.1.8 Cyber Situation Awareness

It is increasingly important to understand the actual state of Cyber elements of the Space Segment during operation, including the presence of Cyber intrusions or attacks, if they are underway. Most available mechanisms to support Cyber Situation Awareness (Cyber SA, CSA) will focus on the interfaces of the space vehicle with ground control and user equipment.

But Space Segment capabilities (whether through Space Vehicle (SV) or through payload mechanisms) may also be exploitable. Advanced persistent threats may be able to exploit weaknesses in the protection of the state and the computation on board Space Segment assets. These exploitations may arise from zero-day flaws, possibly introduced maliciously or accidentally at some point(s) in the bus and payload hardware, firmware and software development supply chain, or they may be introduced (again either maliciously or accidentally) through improperly managed updates/patches during operations, such as those addressed in Guideline 7-6.

The ability to use reliable capabilities on the SV to enable detection and reporting of intrusions may require new architecture, design, and implementation features that may be cost prohibitive for heritage programs. Nevertheless, it may still be possible to re-purpose for Cyber SA some capabilities already provided on legacy/heritage platforms. For example, command count tracking and validation designed for launch and early orbit processing checkout may be used to detect covert adversarial commanding.

Guideline 7-8. Establish and maintain continuous Cyber Situation Awareness

Recommendation:

- Establish monitoring procedures based on existing capabilities in the space segment implementation.
- Where possible, monitor Space Segment software and firmware for inadvertent changes during operations, using techniques such as:
 - periodic validation of operational software/firmware signatures, per Guideline 6-21;
 - control-flow monitoring to detect anomalous SW execution patterns.

Evaluation Criteria: Capabilities provided by the existing space segment implementation provide basis for monitoring for cyber events. For example, continual evaluation of Space Vehicle telemetry might provide insight to adversarial or malicious commanding, configuration changes, state changes.

Milestone: Continuous capability throughout operations and sustainment.

Rationale: The principle potential cyber consequences of failure to use existing capabilities to maintain continuous Cyber SA include the inability to detect and respond to Space Cyber attacks, or cyber events of inadvertent or erroneous origin, before they cripple mission effectiveness.

For some heritage systems, identifying and monitoring of Space Vehicle telemetry streams that were initially instrumented for hardware/software failure detection may enable the capture of unexpected configuration, state or command changes pertinent to Cyber situation awareness.

For systems under new development, more advanced techniques may be feasible such as operational signature validation, or ground model-based control-flow monitoring to detect anomalous execution patterns.

Stakeholders/Actions:

- FFRDC/Overseeing Organization/Program Office: Evaluate Space Vehicle instrumentation for application to Cyber SA purposes. Develop new system (or heritage system upgrade/recap) requirements for future development to enhance real-time Cyber SA capabilities.
- System operator: Implement Ground procedures to monitor unexpected vehicle changes and application to Cyber SA.
- System operator: Evaluate and report on unexpected vehicle changes and potential relevance to Cyber SA.

7.1.9 Cyber Response Capability Enhancement

Conducting periodic threat, vulnerability, and mitigation reassessments (per Guideline 7-7) , and attempting to use existing capabilities to provide continuous Cyber SA (per Guideline 7-8) will produce considerable understanding about the kinds of situations likely to arise for which the current mechanisms are inadequate for competent threat response at netspeed.

From this understanding, analysis of alternative development options can be conducted for the next recapitalization cycle, and analyses/trades of risk (performance, cost, etc.) against operational benefit can be used to ensure that recapitalization events produce affordable improvements in mission resilience. This guideline implies the use of Guideline 6-11.

Guideline 7-9. Refresh Cyber Response Capabilities

Recommendation: When developing system upgrade needs and conducting trades of alternative developments to meet those needs, include as critical drivers

- capabilities in support of Cyber SA and
- countermeasures to improve mission resilience.

Evaluation Criteria: Periodically assess and identify Cyber Response improvements to changing threat surfaces and threat initiatives.

Milestone: Throughout operations and sustainment.

Rationale: For mission resilience and Cyber situation awareness, it is essential to include both Cyber SA and countermeasures as drivers in considering the opportunity for improvements through ground system recapitalization. These evolve rapidly: over the lifecycle of the Space segment solution, change will be observed not only in mission functional and resilience needs, but also in threat initiatives and threat surfaces.

Stakeholders/Actions:

- FFRDC/Overseeing Organization/Program Office: Rank Cyber SA and mission resilience highly among the factors to be considered when nominating and evaluating system improvements for funding.
- System operator: Identify Cyber SA and mission resilience needs.
- Contractor: Identify and evaluate means to satisfy Cyber SA and Mission resilience needs .

7.2 Protecting Space Programs in Operations

In addition to improving the security practices of space system operations centers it is also necessary to continue protecting critical program information, technologies, and components (designated by the term “artifacts” herein). As discussed in section 5.3, this activity falls under the umbrella of program protection and the normal Program Protection Plan (PPP). However, program protection is often inadequately done during operations, despite the need for improved program protection due to the escalating threat environment. It is essential that the enhanced program protection as provided in Guideline 5-1, Guideline 6-12, and Guideline 6-13 be continued in the operations of new and heritage programs.

Guideline 7-10. Implement enhanced Program Protection Planning during operations

Recommendation:

- Based on current intelligence, technology, and operational environment assessments, update critical program information, technology, and components to be protected during operations.
- Review and update operational program protections practices per the updated assessment.

Evaluation Criteria: Stakeholder concurrence that important program information is adequately protected via review of developer accountability documentation PPP.

Milestone: Throughout operations and sustainment.

Rationale: Protection of key technologies, components, and information systems is necessary throughout the program lifecycle to prevent subversion of the information system, the mission information it provides/manages, and ultimately the mission itself.

Stakeholders/Actions:

- AO/Overseeing Organization/Program Office: Establish a threshold of risk that is acceptable for critical program artifacts. Fund the mitigation actions for those that address unacceptable risk.
- FFRDC/Overseeing Organization/Program Office: Establish program policy for information repository and program interchange protections by all operational program participants. Update the Program Protection Plan (PPP) identifying critical program artifacts for mission success.
- Contractor: Update PPP, detailing planned implementation of the defined policy, information, and technologies. Implement necessary technical measure protection mitigations.
- System Operator, User: Contribute mission operations perspective to PPP and implement applicable protection procedural mitigations.

8. Unresolved Challenges/Future Work

This Guide has emphasized the rapid change the NSS-S community is undergoing in its response to the challenge of achieving mission assurance and continuity despite its dependence on the actively contested domain of Cyberspace. This chapter addresses some of the important areas in which to expect that change to result in new practices, new products, and new organizational structures for NSS-S mission operations. These are areas in which it is premature to provide explicit guidance today, and for which it may be appropriate to develop a sequel to this Guide.

Here is a short list of topics that will influence information assurance and cyber security practices in the future:

- Use of commercial space technologies.
The NSS-S community already employs the use of commercial space assets, and is likely to expand both the degree and the nature of such usage. The need to address the cyber security aspects of such use is becoming more apparent, and the expansion of dependence upon such assets will only heighten that need.
- Iteration of TOR-2007(8583)-6702 for the NIST SP 800-53 controls.
The TOR-2007(8583)-6702 guidance for application of the DOD 8500.2 controls to space systems needs to be updated to the merged guidance of NIST SP 800-53 for application to Intelligence Community and other Federal space systems. An effort is now (Spring 2011) underway at The Aerospace Corporation³⁶ to do this extension.
- Supply Chain Risk Management (SCRM) application beyond Application Specific Integrated Circuits (ASICs).
To be effective SCRM must apply not only to the procurement of hardware (e.g., ASICs) from trusted foundries, but also FPGAs, Intellectual Property (IP) cores for incorporation into ASICs or FPGAs and the procurement of Free Open Source and COTS SW. In Spring 2011, OSD is conducting a major initiative in this area. But in the long run, even more will be required to provide for mission resiliency.
- Enhanced Program Protection.
Specific guidance for enhanced Program Protection is needed across the DOD, IC, and Federal communities, but NSS-S has unique exposure and needs for enhanced Program Protection due their complex and lengthy procurement cycles and longevity of service. In Spring 2011, OSD is conducting a major initiative in this area. But in the long run, even more will be required to provide for mission resiliency.
- Cyber Resilience Documentation.
Artifacts implied by the cyber resilience activities outlined in chapter 4 should ideally be captured in existing program documentation. A listing of the necessary documentation for cyber resilience, the originator and appropriate document to capture each artifact should be generated.
- IA evaluation methods for Space Segment non-developed items and other components.
Satisfaction of IA-related goals, objectives, and requirements must often realistically be accomplished by non-IA systems or system components, including re-used COTS/GOTS/FOSS products. Consequently, guidance is needed for process and best-practices to ensure that IA-related goals, objectives and requirements are properly flowed-down and verified even when all (or a portion) of that capability is ultimately accomplished by a non-IA specific system or system element.

³⁶ Daniel Faigin is leading / conducting this effort.

- Guidance for System Engineering on process for integrating both technical and non-technical IA Controls.

Current system engineering processes are geared towards allocation of functional and technical requirements within a system architecture. IA controls on the other hand constitute a mix of management, operational, and technical controls consistent with the “defense-in-depth” approach that integrates people, technology, and operations as a means for mitigating IA risks. This introduces a unique challenge for system engineers when flowing down IA requirements. Further work is needed to develop guidance on how to integrate the flowdown of both technical and non-technical IA controls within the System Engineering process. The guidance should also address the difference in flowdown of IA controls that are considered as security features built into the system being delivered vs. the IA controls that are required to protect critical program information during system development.

- Authorizing Official (AO) Involvement Throughout the Acquisition Process.

As mentioned earlier in this report, it is ideal that the Authorizing Official be involved in system security decisions throughout the SDLC so that the achievement of successful C&A does not become a stumbling block. Defining a set of specific IA deliverables and process that requires Authorizing Official sign-off or formal concurrence at each acquisition phase or milestone needs to be examined if it is feasible and if it would encourage Authorizing Official involvement.

Appendix A. Risk Management Framework – Primer

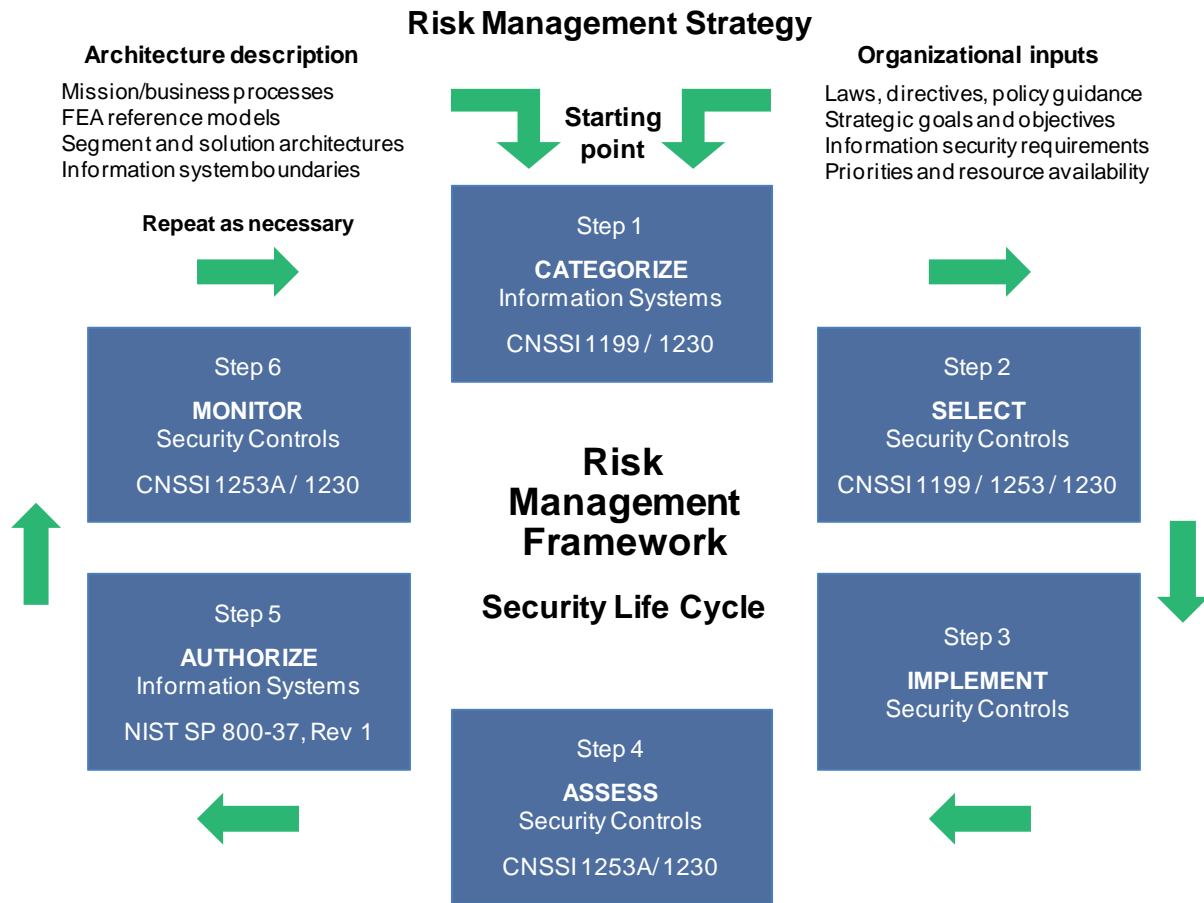


Figure A-1. Risk management framework security lifecycle.

Step 1. Security Categorization

Security Categorization (SC) is the starting point and foundation of the Risk Management Framework. This step involves assessing the impact of loss of confidentiality, integrity, or availability on the mission, business, or enterprise. Senior agency and program officials meet to establish the security categorization (SC) value for a system to select the baseline security controls that will be incorporated into a system's baseline requirements.

The baseline method of security categorization is a three-step process:

Step 1 Security categorization of information types. [What kind of information does the system process?]

Step 2 Security categorization of NSS using the output from Step 1. [Select baseline security control requirements from the NIST 800-53-based security control catalog.]

Step 3 Risk adjustment of the NSS categorization using the output from Step 2 as a starting point. [Review security scoping and select security control enhancements as necessary to protect the agency's mission fulfillment.]

In accordance with CNSSI 1253 “*Security Categorization and Control Selection for National Security Systems*” (www.cnss.gov) all information types processed by a National Security Systems (NSS) must be reviewed for potential impact of loss on confidentiality, integrity, and availability. The information type review must consider all factors that may affect an organization’s mission, business objectives, and system risks. Each system’s information type(s) must be reviewed independently and must take a look at a micro and macro view of the system and related mission objectives. Acceptable impact values are Low, Moderate, and High.

The standard SC format for an information type is given as follows:

SC information type = {(**confidentiality**, *impact*), (**integrity** *impact*), (**availability** *impact*)}

The security categorization of the system is similarly given as:

SC_{NSS} = {(**confidentiality**, *impact*), (**integrity** *impact*), (**availability** *impact*)}

The potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) will be the highest values from among those security categories that have been determined for each type of information resident on the NSS. The values of each security objective comprise the base security categorization of a system. Organizations must consider operational or environmental factors that might mitigate or increase the potential impact of loss of C, I, or A on the organization or agency mission. A risk-based adjustment on the systems’ security categorization can be made after considering the specific factors. If the final security categorization is changed based on a risk-based adjustment, it is stated as:

SC (post-RA)_{NSS} = {(**confidentiality**, *impact*), (**integrity** *impact*), (**availability** *impact*)}

Security control selection can be based on categorized potential impact levels (as described above) or through the use of control profile security categorization used when enterprise-level considerations involve the security management of multiple systems in the same or similar manner to meet mission needs.

Step 2. Security Control Selection

Security controls, including control enhancements, and agency- or mission-area specific security controls are selected commensurate with protecting confidentiality, integrity, and availability at the mission, business, or enterprise area. This is an important step following SC to ensure that appropriate security control requirements are incorporated into the system baseline and “built-in” and tested repeatedly during the SDLC. As with SC, this step occurs early in the development lifecycle to maximize value and minimize potential costs. Legacy or operational systems may be required to assess their SC to ensure so that agency officials can assess any gaps that may exist between required security controls and those currently implemented in the operational systems. Further, they may choose to retrofit system elements with appropriate security controls as applicable and possible, for space segment systems.

After establishing the system’s security categorization, security controls are selected, tailored, and supplemented using the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security control catalog. Controls should be selected in accordance with the impact levels recorded in the security categorization step. If a control profile is used, organizational guidance regarding the specific control profile, including whether tailoring or supplementing is permitted, is used. The CNSSI-1253 provides: guidance on tailoring controls due to operational considerations;

scoping guidance based on system mobility, physical hosting environment, system capabilities or technologies, and processing and storage capabilities; supplemental controls due to inadequate risk mitigation by tailored security controls.

Step 3. Control Implementation

This step involves implementing selected controls and control enhancements in systems. Create/update a security plan that describes how controls are implemented within the operating environment. This step helps to substantiate decisions made on security requirements, enhancements, scoping, and common controls. It gives a clear view to team members and testers about how a system is protected.

Step 4. Control Testing and Assessment

This step involves assessing the system's implemented security controls using tailored assessment procedures to validate that the security controls are implemented correctly, operating as intended, and meeting the security protection requirements for the system. This step also validates security control decisions up to this point and provides an opportunity for security testers to take a fresh look at the systems protection mechanisms. The testers control review provides evidentiary artifacts and the basis for recommending or not recommending a system for authorization/accreditation.

Step 5. Authorization

This step involves a senior agency official or Designated Approval Authority (AO) making a decision to accept or reject a system's request for authority to operate. Because senior agency officials are involved early in the risk management framework, officials are much more familiar with systems and better equipped to make informed decisions on accepting risk, spending more money and time on protective controls, and understanding the impact of loss of C, I, or A on the agency's mission.

Step 6. Continuous Monitoring

After a system is authorized by the AO to operate the last risk management framework step, continuous monitoring, goes on in perpetuity for as long as a system is authorized and operational. This step serves to ensure that system security controls always meet or exceed the benchmarks established in the previous steps. Continuous monitoring also serves as a barometer for measuring, detecting, and responding to changing conditions, including emerging threats and vulnerabilities. If gaps in security protection occur as a result of emerging threats, changing environmental conditions, or through carefully planned and approved configuration-controlled changes, continuous monitoring is the tool that will alert system owners, managers, and operators to start another cycle through the risk management framework. When impactful changes are detected in an operational environment, additional or modified security controls may be selected, modified, implemented, tested, and authorized to ensure that the system maintains a security posture that is commensurate with the impact of loss of mission capability to the agency. Vigilance through continuous monitoring is one of the most important steps in the Risk Management Framework to ensure that systems supporting critical mission activities are protected and can prevent, anticipate, and respond to changing threats.

Appendix B. Guideline Cross-Reference Matrix

This appendix provides cross-reference tables as an aid for the reader to correlate guidance from one phase or perspective to another. For convenience of representation this information is split into two tables with sections 3, 4, 5 and 7 cross-referenced to all of sections 3 through 7 in Table B-1 and section 6 cross-referenced to sections 3, 4, 5 and 7 in Table B-2. In both tables the rows represent the “from” guideline and the columns the “to” guideline. They are generally symmetric and bi-directional, with a few exceptions due to a guideline in one section only addressing a portion of the scope of that in the other. Note that an “X” in a cell indicates cross-references between guidelines.

Table B-1. Guideline Cross-Reference from Sections 3-7 to Sections 3-5, 7

F\T	3-1	4-1	4-2	4-3	4-4	4-5	5-1	5-2	5-3	5-4	7-1	7-2	7-3	7-4	7-5	7-6	7-7	7-8	7-9	7-10
3-1								X		X	X									
4-1								X											X	
4-2								X					X							
4-3								X											X	
4-4								X										X		
4-5								X											X	
5-1																				X
5-2	X	X	X	X	X	X														
5-3																				
5-4	X										X									
6-1								X												
6-2												X								
6-3																				
6-4																				
6-5																				
6-6										X	X									
6-7	X									X										
6-8																				
6-9																				
6-10																				
6-11																		X		
6-12			X				X													X
6-13			X				X													X
6-14		X																		
6-15			X					X					X							
6-16				X																
6-17		X		X				X										X		
6-18					X			X										X		
6-19						X		X												
6-20															X					

F/T	3-1	4-1	4-2	4-3	4-4	4-5	5-1	5-2	5-3	5-4	7-1	7-2	7-3	7-4	7-5	7-6	7-7	7-8	7-9	7-10	
6-21																					
6-22																					
6-23																					
6-24																					
6-25																				X	
7-1	X									X											
7-2			X																		
7-3																					
7-4																					
7-5																					
7-6																					
7-7																					
7-8						X															
7-9		X		X		X															
7-10							X														

Table B-2. Guideline Cross-Reference from Sections 3, 5, 7 to Section 6

F/T	6-1	6-2	6-3	6-4	6-5	6-6	6-7	6-8	6-9	6-10	6-11	6-12	6-13	6-14	6-15	6-16	6-17	6-18	6-19	6-20	6-21	6-22	6-23	6-24	6-25
3-1							X																		
4-1														X			X								
4-2												X	X		X										
4-3															X	X									
4-4																		X							
4-5																			X						
5-1												X	X												
5-2																									
5-3																									
5-4						X	X																		
7-1						X																			
7-2		X																							
7-3														X											
7-4															X										
7-5																					X				
7-6																									
7-7																									
7-8												X					X	X							
7-9																			X						X
7-10												X	X												