Cybersecurity for DoD Acquisition Program Execution: Best Practices for the Major Capability Acquisition Pathway

Insights from the Ground Based Strategic Deterrence (GBSD) Program

November 2021

(THIS PAGE LEFT INTENTIONALLY BLANK)

Approved by

GARSTKA.JOH
N.1178095494

Digitally signed by
GARSTKA.JOHN.1178095494
Date: 2021.11.24 13:38:39
-05'00'

24 November 2021

Mr. John J. Garstka
Director for Cyber
Office of the Chief Information Security Officer
Office of the Deputy Assistant Secretary of Defense for Industrial Policy
Office of the Under Secretary of Defense for Acquisition and Sustainment

Date

Cybersecurity Best Practice Guide Change Record

Date	Change	Rationale

(THIS PAGE LEFT INTENTIONALLY BLANK)

FORWARD

Over the past several years the department has made transformative changes to the defense acquisition system by establishing a new acquisition policy eco-system that flows from our national defense strategy and employs an Adaptive Acquisition Framework (AAF) designed specifically for the unique character of our acquisitions. That very substantive department-wide effort resulted in the publication of more than 20 new instructions that detail the policy equities of our partners throughout the Department and specify the revised procedures that govern our acquisitions.

While we can be very proud of those accomplishments, we are sustaining that momentum by developing non-mandatory best business practice that is aligned with the AAF and the newly published functional policies and provides powerful examples of how the new policies can be implemented.

The Cybersecurity business practices discussed in this Guidebook are drawn from experience with the Ground Based Strategic Deterrence Program, an Acquisition Category (ACAT) 1D program leveraging the Major Capability Acquisition Pathway, and are provided with that objective in mind.

INTRODUCTION

The National Defense Strategy and the DoD Cyber Strategy both highlight the imperative for the Joint Force to be capable of operating in a contested cyber environment. The Acquisition and Sustainment community has a key role to play in ensuring the weapon systems meet validated cybersecurity requirements and are cyber hardened to deal with cyber threat presented in Validated Online Lifecycle Threat (VOLT) Reports in compliance with DoDI 5000.90, "Cybersecurity for Acquisition Decision Authorities and Program Managers."

Cyber hardening weapon systems is a daunting challenge for two main reasons. First, program offices have to comply with a lot of cybersecurity policy. By one estimate, there are nearly 23,000 pages of cybersecurity documents that are cybersecurity policies or references to policies[1]. The purpose of this Best Practices Guide is to provide programs with observed effective approaches to complying with DoD policies while also countering the advanced persistent cyber threat. The second challenge is the growing realization that complying with cybersecurity policies is recognized to be insufficient to stop the advanced persistent cyber threat[2,3] across the DoD.

Therefore, this Best Practice Guide takes a different approach than past cybersecurity guidebooks. It examines and describes best practices from the Ground Based Strategic Deterrent (GBSD) program, based on its reputation for embracing "above and beyond" practices in order to build a system resilient to the advanced persistent cyber threat. The GBSD weapon system is being developed to eventually replace the Minuteman III Intercontinental Ballistic Missile program. It is located within the Air Force Nuclear Weapon Center. The GBSD program is an Acquisition Category (ACAT) 1D program leveraging the Major Capability Acquisition Pathway. Through interviews with GBSD program cybersecurity personnel and reviewing GBSD program produced content, best practices were identified. The best practices were chosen because they are initiatives above and beyond those already required by policies.

Additionally, this guidebook intends to help with the implementation of DoD Instruction (DoDI) 5000.90, "Cybersecurity for Acquisition Decision Authorities and Program Managers." Future versions of this guidebook will provide execution recommendations for the policies and responsibilities captured herein. Program offices can review these best practices and select what may work for them given their respective acquisition pathway and phase. Each best practice includes a few key points, followed by a case study for most of the best practices. Future versions of guidebook will also expand upon the set of best practices to include those from other DoD programs. The Cyber Directorate in the Office of the Under Secretary of Defense (OUSD) for Acquisition & Sustainment (A&S) would like to hear of other best practices across the DoD for inclusion in the next update to this guide. Please send ideas to osd.mc-alex.ousd-a-s.ciso-cyber-team@mail.mil.

[1] Patch, Cully, Cyber Security & Information Systems Information Analysis Center (CSIAC), Personal Correspondence, 24 November 2020.

[2] DoD Cybersecurity Test and Evaluation Guidebook version 2.1, 10 February 2020, https://ac.cto.mil/dte/cyber/

[3] Joint Staff, Cyber Survivability Endorsement Implementation Guide, 2019

Table of Contents

Page

1. CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS (CROWS)

Service Level Cybersecurity Help
DOTMLPF: Organization

1.1 KEY POINTS

- CROWS is a service level organization in the Air Force's Life Cycle Management Center dedicated to helping program offices "bake-in" cyber resiliency into weapon systems in acquisition and sustainment.

- CROWS produces the Systems Security Engineering Cyber Guidebook[4] (SSECG) and updates it on a frequent basis to provide information on how to perform Systems Security Engineering (SSE) in a way that complies with Federal, Department of Defense, and Service-level policy

- Rather than establishing lists of cybersecurity practices and processes and assigning them to key acquisition milestones for compliance, the CROWS is working to integrate cybersecurity thinking, design constraints, and decision making into existing systems engineering processes

- CROWS established an education and training team that is a resource to Air Force programs and individual SSEs

1.2 CASE STUDY

The CROWS SSECG begins with a decomposition of much of the nearly 23,000 pages of weapon system cybersecurity policy, created through the US government's attempts to help make weapon systems more secure from cyberspace threats. Traditional systems engineers who are new to the cyberspace arena may find the sheer volume of guidance and material particularly daunting, and as discussed in the introduction to this guidebook, compliance schemes are unlikely to thwart the advanced persistent threat. The CROWS SSECG provides much needed guidance to the SSE process to help meet the requirements of regulation. The GBSD program office used the CROWS SSECG in the process of preparing the EMD Request For Proposal (RFP)

The SSECG then provides content on how to do the work of SSE for cyberspace. The SSECG provides a roadmap to comply with policy and regulations and develop the artifacts necessary to support many different documents such as:

- The System Requirements Document (SRD)
- System Specification (to include test)
- Statement of Objectives (SOO)

[4] USAF CROWS Systems Security Engineering Cyber Guidebook, Version 3.0, 2020, http://acqnotes.com/wp-content/uploads/2020/12/SSE-Cyber-Guidebook-v3.0-5-Nov-2020.docx

- Statement of Work (SOW)
- Contract Deliverable Requirements List (CDRL)
- Section L, and Section M for the Request for Proposal (RFP)
- Program Protection Plan (PPP)
- Cybersecurity Strategy
- And others

The SSECG provides the starting point for program offices to engineer resilient systems and then navigate through the myriad of policies and processes required for compliance as an output of the engineering process.

The CROWS SSECG also offers a sample Work Breakdown Structure (WBS) for the USAF SSE Cyber Workflow Process. This is a great tool to integrate cybersecurity into the larger systems security engineering and systems engineering processes. As program offices make cybersecurity part of the regular systems engineering process, cybersecurity should become less of a compliance-driven activity and more of an engineering activity tailored to meet the needs of the program.

1.3 EDUCATION AND TRAINING

The CROWS office established a training and education pipeline. The training and education pipeline will allow individuals to complete a worked example where they will have the opportunity to produce cybersecurity requirements, a cybersecurity strategy, and a test and evaluation master plan. These documents will be available as a resource for their programs of record. Training and education will aid in producing the next generation of cybersecurity engineers.

2. CYBERSECURITY REQUIREMENTS

Developing Requirements for a Capability Development Document (CDD)
DOTMLPF: Doctrine

2.1 KEY POINTS

- The Risk Management Framework (RMF) does not have a process to establish mission-based cybersecurity requirements

- GBSD program took the lead to develop the first ever set of cybersecurity requirements based on a matrix of deliberate cybersecurity threat events and *access vectors* instead of existing cybersecurity policies

- The GBSD program recognized that cyber threats may evolve over time, but CDDs cannot, and therefore today’s weapon systems must be designed to be resilient to future threats

- Joint Staff Cyber Survivability Attribute (CSA) compliant – Joint Requirements Oversight Council (JROC) approved

2.2 CASE STUDY

The Risk Management Framework is one document in a series developed as part of the response to the Federal Information Security Modernization Act (FISMA). Federal Information Processing Standard (FIPS) 199 describes standards for categorizing federal information if a system has a high, medium, or low risk to confidentiality, integrity, and availability. FIPS 200 outlines the minimum-security requirements for federal information and information systems. NIST SP 800-37 describes the RMF, which “provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.”[1] NIST SP 800-53 is the source of security controls for NIST SP 800-37 and these controls are intended to meet the requirements in FIPS 200. Although RMF Step 1 requires engineers to categorize the sensitivity level in accordance with FIPS 199 and CNSSI 1253, it does not have a process to establish mission-based cybersecurity requirements. Therefore, the RMF does not have a requirements generation phase.

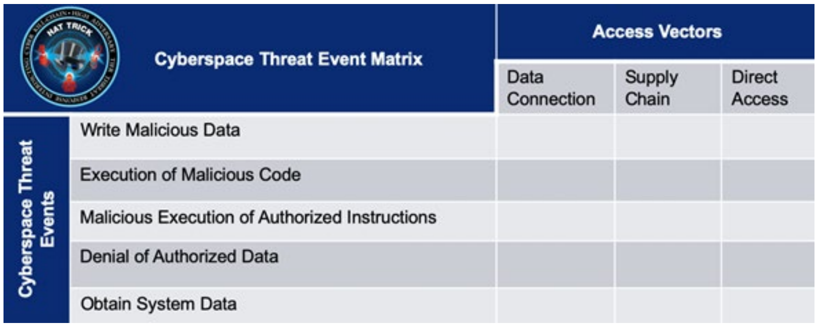
> *“The RMF process will inform acquisition processes for all DoD IT, including requirements development, procurement, and both developmental T&E (DT&E) and operational T&E (OT&E), but the RMF process does not replace these processes.” – DoDI 8510.01*

A search for the word ‘requirement’ in the Department of Defense Instruction (DoDI) 8510.01 results in at least eight specific references in the document that state requirements should be generated independently of RMF. A great example comes from paragraph 3.k. of the document, which states that "the RMF process will inform acquisition processes…including requirements development…but does not replace these processes."[5]

2.3 DESIGN TODAY FOR TOMORROW'S CYBERSPACE THREAT

The requirements in FIPS 200 are the minimum for federal information and information systems (i.e. enterprise information technology). These requirements are not intended to keep the highest tier adversaries from impacting our national security systems. In fact, RMF explicitly excludes national security systems. CNSSI 1253 modifies the FIPS 199 categorization, uses the NIST SP 800-53 controls, creates overlays of those controls, and authorizes the use of RMF for national security systems. Tragically, these controls and overlays often become the cybersecurity requirements for our national security systems. This is tragic because controls are supposed to be used to *meet* requirements, not to *be* requirements themselves.

The GBSD program took a fresh approach. They wanted to build the GBSD weapon system today to be resilient to tomorrow's cyberspace threats by giving GBSD operators a system that could fight through cyberspace attacks and still perform its mission. To do this, the program had to determine how to characterize the cyberspace threat in a way that would not need to change much over time. The cyberspace threat events were decomposed into access vectors any adversary must use and the threat events that are the building blocks for any cyberspace attack (Figure 2-1). If these threat events can be prevented, then the system will be able to prevent any adversary, including the highest tier adversaries with zero-day exploits, from achieving their objectives. Based on this threat event matrix, the GBSD program wrote requirements to prevent, detect, and respond to these threat events from these access vectors. GBSD is the first DoD program to take this approach to defining engineering requirements that are mission-relevant and measureable.



Cyberspace Threat Event Matrix		Access Vectors		
		Data Connection	Supply Chain	Direct Access
Cyberspace Threat Events	Write Malicious Data			
	Execution of Malicious Code			
	Malicious Execution of Authorized Instructions			
	Denial of Authorized Data			
	Obtain System Data			

Figure 2-1. Cyberspace Threat Event Matrix

Cybersecurity Technical Performance Measures (TPM) were provided as part of the requirements process and documented in the Systems Engineering Plan (SEP). The TPMs allow the program office to monitor the progress of the performer in meeting the resilience criteria set for each access vector.

[5] DoD CIO, "DoD Instruction 8510.01", 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

2.4 JOINT STAFF SURVIVABILITY KEY PERFORMANCE PARAMETER

The cybersecurity requirements generated for the GBSD weapon system had to clear the hurdle of the Joint Staff Cyber Survivability Endorsement Implementation Guide. These requirements met all of the CSAs and received JROC approval.

2.5 GET THE REQUIREMENTS RIGHT

If the requirements are right, everything else falls into place. Capturing well thought out cybersecurity requirements into high-level requirements documents is essential to doing cybersecurity well. Our adversaries change and evolve, but our requirements documents do not.

3. FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTER (FFRDC) AND UNIVERSITY AFFLIATED RESEARCH CENTER (UARC) RESOURCES

Long-term Support Addressing Critical Problems
DOTMLPF: Personnel

3.1 KEY POINTS

- FFRDCs and UARCs provide highly skilled professionals to perform and apply research to address the Nation's most significant challenges

- As not-for-profit entities, FFRDCs and UARCs provide services unbiased by profit motive or shareholder interests

- FFRDCs and UARCs maintain long-term strategic relationships with government sponsors to better meet and anticipate sponsor needs, especially through periods of government leadership turnover and workforce attrition

3.2 FFRDCS AND UARCS

A UARC is a research organization supporting the DoD and is associated with a specific university. UARCs may compete for science and technology work, unless precluded from doing so by their DoD contracts. Generally, UARCs may not compete against industry in response to competitive Requests for Proposals (RFPs) for development or production that involve engineering expertise developed or sustained through contracts awarded under 10 U.S.C. 2304(c)(3)(B).[6] FFRDCs are private-run research organizations that receive direct funding from the government. FFRDCs are not allowed to compete for work with other private sector organizations.[7]

Both UARCs and FFRDCs provide cutting-edge technical and scientific support in a flexible way that the government can leverage for both short-term and long-term needs. These research organizations are valuable repositories of up-to-date operational experience with broad access to sensitive and proprietary information that can be implemented quickly to meet evolving strategic and operational needs. As providers of technical expertise, both UARCs and FFRDCs have a mandate to maintain the level of engineering, research, and development capabilities required to meet the needs of their government sponsors at a moment's notice. The technical memory UARCs and FFRDCs provide persists through government leadership turnover and attrition of key science and engineering leaders to help ensure long-term success in strategy.

[6] Director of Defense R&E, DoD University Affiliated Research Centers (UARC) Management Plan, 2010, https://rt.cto.mil/wp-content/uploads/2019/09/UARC-Mgmt-Plan-Jun-23-10-FINAL-6811-with-Signed-Memo.pdf

[7] MITRE, "FFRDCs—A Primer: Federally Funded Research and Development Centers in the 21st Century", 2015, https://www.mitre.org/sites/default/files/publications/ffrdc-primer-april-2015.pdf

The GBSD program makes extensive use of FFRDCs and UARCs to staff system development and security engineering positions to include cybersecurity. These experts are already aware of GBSD special needs, as well as general technology and security trends, and provide insights to produce a secure and functional system design for the GBSD weapon system. The director of the GBSD Systems Directorate regularly highlights the critical contributions FFRDCs and UARCs make that are improving the GBSD program.

4. INTELLIGENCE DIVISION

Organic Intelligence Support Synergizes Intelligence Community Partners
DOTMLPF: Organization

4.1 KEY POINTS

- An organic intelligence support organization within the program office maximizes intelligence that informs all aspects of the acquisition lifecycle

- Intelligence analysts imbedded with the acquisition program are uniquely positioned to have deep understanding of the weapon system and acquisition program details and can therefore craft intelligence collection and reporting requirements well suited for systems engineering and programmatic decision making

4.2 CASE STUDY

The director of the GBSD Systems Directorate decided to formally establish an intelligence division as a direct report after Milestone B. The director charged the division with "providing full spectrum intelligence support to the design, test, manufacturing, deployment, and sustainment of DoD's next generation nuclear deterrent."[8]

The new division immediately set out with the following goals:

- Establish a cyber-threat intelligence process to include creation of Cybersecurity Critical Intelligence Parameters (CIPs) and similar production requests (PRs) or collection requirements

- Fully test supplier vetting process as part of a larger Supply Chain Risk Management program

- Establish fully operational Secure Compartmented Information Facility (SCIF) within the program office's spaces

- Organize bi-annual intelligence working groups with prime contractor

- Host weekly intelligence exchanges with prime contractor

- Conduct regular interactions with key partners across the intelligence community

- Integrate intelligence with all other program office divisions

- Continue to host Strategic Deterrence Intelligence Summit

[8] Andrew Rodriguez and David Sawyer, "GBSD Mission Defense & Intel", 2020

This division has a mix of government civilian, Integration Support Contractor (ISC), and FFRDC/UARC support. FFRDCs and UARCs have unique capabilities to augment intelligence with technical analyses of adversary capabilities. The intelligence division regularly takes advantage of these capabilities to improve the design of the weapon system.

5. MISSION DEFENSE UNDER SYSTEM ENGINEERING

Integrating Cybersecurity and Other Security Disciplines in Systems Engineering
DOTMLPF: Organization

5.1 KEY POINTS

- Organizing all security disciplines in one organization maximizes synergy
- Placing the Mission Defense Branch under the Systems Engineering Division ensures security is intrinsic to the weapon system in acquisition

5.2 CASE STUDY

The GBSD Program Management Office made a decision early in the acquisition cycle (Milestone A) to establish a Mission Defense Branch underneath the Systems Engineering Division. Aligning the Mission Defense Branch under the main Systems Engineering Division smooths the way for the program office to integrate all security disciplines and makes security organic to the division responsible for leading the engineering of the weapon system.

The Mission Defense Branch contains the security disciplines of Nuclear Surety, Cybersecurity, Supply Chain Risk Management (SCRM), System Safety, and Program Protection. This alignment sets up the opportunity for greater interaction between these security disciplines, which would otherwise be at risk for operating as independent security stovepipes if organized haphazardly in a program office.

The Risk Management Framework set of controls from NIST 800-53 includes non-cybersecurity controls like physical security, SCRM, etc. Therefore, organizing the security disciplines under a single branch enables synergy in support of RMF.

This organizational schema integrates most security disciplines enumerated in DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage"[9]. This enables the GBSD program to meet the policy objectives of this DoD instruction. In the case for the GBSD program, Software Assurance is a sister branch to the Mission Defense Branch under the Systems Engineering Division. This separation of the Software Assurance discipline from the other security disciplines is due to the sheer size of the software effort for the GBSD program.

Additionally, GBSD prioritized organic UARC/FFRDC support inside the Mission Defense Branch to leverage their unique capabilities. See other best practices.

[9] OUSD R&E, "DoD Instruction 5000.83", 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf

6. MISSION DEFENSE OPERATIONS CENTER (MDOC)

Central Cybersecurity Operations Management for the Program Office
DOTMLPF: Organization

6.1 KEY POINTS

- MDOC is the cybersecurity authority responsible for protecting the GBSD weapon system
- The consolidated cybersecurity resources working together provide ongoing support to meet the needs of the program from start to finish
- Creating the MDOC during the early stages of system development ensured better protection of GBSD system resources

6.2 CASE STUDY

The GBSD program provides modernized nuclear capabilities to replace aging Minuteman III Intercontinental Ballistic Missiles (ICBM).[10] The program created the MDOC as part of the material solution analysis phase of product development to protect the program's critical resources. Too often programs fail to consider processes, procedures, and technologies for Defensive Cyber Operations (DCO) and active defense during capability identification. Deferring these considerations to the Production & Development or the Operations & Sustainment phases of the acquisition lifecycle leaves a period of time during which the developing systems can be targeted by adversaries before any defenses are in place. The GBSD program recognized that active defense constitutes a critical program requirement and that MDOC planning should begin with Material Solution Analysis. This early lifecycle standup enabled the MDOC to protect the development and deployment of GBSD systems, ensuring adversaries had no window during which GBSD systems were undefended.

The early creation of the MDOC in the system development cycle allowed for closer integration of the MDOC with the systems it secures. The MDOC provides active defense of GBSD systems, including ongoing red team exercises and blue team hunting activities. By standing up the MDOC early in the system development lifecycle, the GBSD program brought these active defense capabilities online during the development of the systems the MDOC defended. This addressed the ability of the adversary to "shift left" in their effect development and protected the system earlier in the system lifecycle.

Centralizing cybersecurity responsibility for the program maximizes unity of effort, minimizes friction, and creates a touchpoint for coordinating cybersecurity efforts with external organizations. It also provides an environment to train the cybersecurity professionals needed to protect the program and to grow a culture of cybersecurity awareness throughout the program. The MDOC provides a key tool for the GBSD program to organically implement cybersecurity activities outlined in DoDI 8530.01. Additionally, when support from the greater cyberspace operations community is necessary, the MDOC provides the GBSD program a centralized body to manage supported cybersecurity response actions.

[10] Northrop Grumman, GBSD, https://www.northropgrumman.com/gbsd/

7. RED TEAM EXERCISES

Adversarial Verification of Security
DOTMLPF: Doctrine

7.1 KEY POINTS

- Red team exercises identify vulnerabilities in the system while verifying the security requirements of the system are sufficient for the level of threat the system is expected to face

- Red team exercises provide a valuable check on the design and security of a system

- Red team exercises are highly flexible and can be performed throughout the system lifecycle

- Management should prioritize iterative red team exercises throughout the product lifecycle

7.2 WHAT IS A RED TEAM EXERCISE?

A red team exercise involves a group of trusted cybersecurity attack experts known as the "red team" performing a simulated or real/actual attack on a system in an effort to mimic the types of attacks a real-world adversary could use. The red team carefully tracks the attacks they used, what the impact of those attacks were, and provides a report of the results to the system owner. The red team may also provide a list of suggested mitigations that address the identified issues. A cybersecurity defensive blue team may work to defend the system in real time during the red team exercise to give a better sense of how the system would perform in a real-world attack scenario. The majority of red team exercises find security weaknesses in the system under test.[11] Red team exercises help identify cybersecurity failures prior to deploying a system in an environment where such a failure could have disastrous consequences.

Red team exercises are contractor performed developmental test events serving as contractor Adversarial Cybersecurity DT&E (ACD) as described in the DoD Cybersecurity Test and Evaluation Guidebook, and DoDI 5000.89 Test and Evaluation. DoDI 5000.75 states that ACD is a required activity in the testing plan to verify system survivability and operational resilience. Red team testing, red teaming, purple teaming, cyber tabletop testing, and adversarial assessment are phrases that are used to describe a wide range of different activities in which a trusted party simulates a real-world threat to the system. These exercises range from table-top exercises to identify and strengthen areas of a system design likely to be targeted by an adversary prior to system development (cyber table top exercises) to official adversarial testing involving highly skilled red and blue team staff in a no-holds-barred contest to identify any possible system weakness in the finished system (adversarial assessment). Because the red team coordinates with the system owner to establish their approach to attacking the system, each red team test plays out differently.

[11] Exabeam, "Study Reveals 62% of Blue Teams Struggle to Catch Red Teams in Adversary Simulation Exercises", 2020, https://www.exabeam.com/newsroom/study-reveals-62-of-blue-teams-struggle-to-catch-red-teams-in-adversary-simulation-exercises/

7.3 RED TEAM EXERCISE WEAKNESSES

Red team exercises are being increasingly requested as their utility and value to system security have been recognized by a wider audience; however, military test organizations are indicating a critical need for more red team staff.[12,13] This poses a significant problem as the highly qualified staff needed to support red team exercises are not easy to find or train and government and military organizations continue to struggle to retain high value cybersecurity staff.[14]

When purchasing red team services it is important to consider what level of skill is needed and what threats the system needs to be robust against. Contracts for red team exercises may include limits on what the red team can do during the test. Even an experienced, skilled team may provide poor feedback if their ability to target the system is overly limited by contractual obligations. A less skilled red team may fail to identify vulnerabilities in a system due to error, oversight, or lack of ability. However, more experienced and skilled teams will generally cost more and have more limited availability. The quality of the results of a red team exercise are highly dependent on the skills of the team performing the assessment and the degree to which the contract and scope of the test event allow the red team to provide meaningful feedback. Red team exercises are also not holistic. Conducting recurring exercises with diverse teams helps to identify previously overlooked weaknesses and consider previously not considered threat tactics. Follow the DoD Cybersecurity T&E Guidebook to require contractors to conduct ACDs and recurring Mission-Based Cyber Risk Assessments (MBCRA).

Red team exercises are expensive and need to be planned for in advance. Time is needed for testing which may impact system delivery schedules if not planned for in advance. System resources need to be made available for test events, which requires advance planning and coordination. Staff are needed to support test events, write up test reports, and implement any identified changes that need to be made to the system as a result of testing. JHU/APL estimates that an assessment team generally contains 4-10 people, but this number can range much higher for things like cyber table-top exercises that could include over 30 participants.

7.4 RED TEAM EXERCISE CONCLUSIONS

The GBSD program uses ongoing red team exercises as part of the active defense component of the Mission Defense Operations Center (MDOC). In the case of GBSD, the prime contractor and the government are performing red team exercises early to focus on components and sub systems. These recurring MBCRAs enable a mission focus to prioritize weaknesses and vulnerabilities in the design. Hands-on threat representative testing (ACDs) will be performed to verify the MBCRA results or the recommended mitigations. This type of ongoing red team exercise provides a constant verification of GBSD systems security. As the red team discovers new vulnerabilities or access vectors, the blue team can immediately provide increased security based on those findings, thereby driving improvements to system

[12] Rachel Cohen, "DOD's Cyber 'Red Teams' Stressed as Security Tests Grow," Air Force Magazine, 2019, https://www.airforcemag.com/dods-cyber-red-teams-stressed-as-security-tests-grow/

[13] Director, Operational Test and Evaluations, U.S. Department of Defense, "2020 DOT&E Annual Report", 2021, https://www.dote.osd.mil/Portals/97/pub/reports/FY2020/other/2020DOTEAnnualReport.pdf

[14] David Vergun, "Recruiting Cyber Workforce Easier Than Retaining Them", U.S. Department of Defense News, 2019, https://www.defense.gov/Explore/News/Article/Article/1955580/recruiting-cyber-workforce-easier-than-retaining-them/

security over time. Red team exercises can help identify vulnerabilities prior to deployment of new systems, identify flaws in the design and implementation of GBSD networked systems, and verify the sufficiency of security and survivability requirements. Red team exercises has significant associated costs in schedule, resources, and money. However, the GBSD program management has determined that the additional cost of ongoing red team exercises is worth the additional security provided. Other programs should consider iterative red team exercises throughout the product lifecycle and allocate program resources accordingly.

8. STPA-SEC

Security by Design
DOTMLPF: Doctrine

8.1 KEY POINTS

- STPA-Sec provides a process for addressing cybersecurity concerns throughout the entire system lifecycle from conceptual development through deployment

- STPA-Sec is already being used to analyze systems and is recognized by industry experts for its effectiveness and ability to create security by design

8.2 CASE STUDY

System-Theoretic Process Analysis for Security (STPA-Sec) is based on System-Theoretic Process Analysis (STPA),[15] which is a process for analyzing system designs for safety concerns based on the System-Theoretic Accident Model and Processes (STAMP) approach to accident analysis. STPA focuses on identifying and investigating the interacting control structures that make up a system to determine which system states will result in a loss of safety. STPA and STPA-Sec are top-down approaches to system analysis that can be performed as early in the system lifecycle as CONOPS development and can iteratively support all stages of the system lifecycle. DoDI 5200.44, "Protection of Mission Critical Functions to achieve Trusted Systems and Networks (TSN)" mandates that acquisition programs conduct "criticality analysis to identify mission critical functions and critical components and reducing the vulnerability of such functions and components through secure system design". STPA-Sec provides program managers a methodology to aid in understanding the impact of system failures stemming from cybersecurity incidents, as well as other adverse events, and therefore provides a way to perform this mandated analysis.

The effectiveness of STPA and STPA-Sec in real-world applications has been the focus of studies and research over the last few years with positive results.[16] Industry leaders have begun to recognize STPA-Sec as a useful tool and have begun to recommend it for government use.[17,18] If implemented early and properly, STPA-Sec has the potential to greatly increase the cybersecurity of future systems.

STPA-Sec expands on the STPA process to specifically address cybersecurity concerns. STPA-Sec analyzes the security impact of the control structures present in a system to identify control actions that, if disrupted or subverted, would lead to vulnerable states in the system.[19] STPA-Sec also includes an adversarial wargaming component (e.g. MBCRAs or table-tops) to help ensure that any weaknesses in the

[15] John Thomas, "Systems Theoretic Process Analysis (STPA)", 2014, http://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Systems-Theoretic-Process-Analysis-STPA-v9-v2-san.pdf

[16] John Thomas and Matt Gibson, "Industry Trials to Evaluate STPA's Effectiveness and Practicality for Digital Control Systems", 2020, http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/Industry-Trials-to-Evaluate-STPA%E2%80%99s-Effectiveness-and-Practicality.pdf

[17] Tom Leighton, "Technology CEOs Share Best Practices with U.S. Government CIOs", LinkedIn, 2017, https://www.linkedin.com/pulse/technology-ceos-share-best-practices-us-government-cios-tom-leighton-1/

[18] IT Alliance for Public Sector, "Tech Industry's Recommendations for Federal IT Modernization," https://www.itic.org/dotAsset/aa5f716a-2fda-474a-95be-c6778f3783a3.pdf

[19] William Young, "STPA-Sec-Tutorial", 2020, http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/STPA-Sec-Tutorial.pdf

system are fully explored. Both traditional STPA and STPA-Sec seek to identify problems as early in the system lifecycle as possible to minimize the investment of both time and resources needed to provide fixes and to increase the impact of those fixes on the safety and security of the end system. STPA-SafeSec[20] is another extension of STPA and STPA-Sec that seeks to integrate these approaches safely and securely, viewing them as a subset of the total emergent properties of the system.

STPA-Sec allows security considerations to be brought into the system development process as early as the conceptual development phase. As a top-down process, STPA-Sec identifies the control structures of the system, defines failure states, and allows for the implementation of any needed constraints and design updates prior to the start of system development efforts. Once system development has started, STPA-Sec can iteratively assess the system implementation, identify control structures, identify insecure control action, and define the security impact of identified actions. Red team activities to determine how an adversary can make use of insecure or missing control actions takes place throughout the system development lifecycle.

Like all engineering processes, STPA-Sec relies on skilled, well-trained professionals to perform the analysis. The staff performing the STPA-Sec process must have a full understanding of the control structures present in the system and have support from the system developers. Good communication between the engineering and development teams is needed to ensure that the design used for the STPA-Sec analysis matches the system implementation and that any changes made to the design are reflected in the system and vice versa. STPA-Sec does not prevent the use of insecure coding methods or vulnerable software and therefore should be used in conjunction with good system development practices as outlined in the USAF SSE Cyber Guidebook.[21]

The GBSD program made use of STPA-Sec to drive security engineering activities as early as the material solutions analysis phase of systems development. Using STPA-Sec allowed GBSD to design systems that minimize security vulnerabilities while meeting program requirements and schedule. The use of STPA-Sec by the GBSD program was indicated by the Office of the Director, Operational Test and Evaluation (DOT&E) as a contributing factor in reducing cybersecurity and schedule risks.[22]

[20] Ivo Friedberg, Kieran McLaughlin, Paul Smith, David Laverty, Sakir Sezer, "STPA-SafeSec: Safety and Security Analysis for Cyber-Physical Systems", Journal of Information Security and Applications (2016), doi: 10.1016/j.jisa.2016.05.008, 2017, https://www.sciencedirect.com/science/article/pii/S2214212616300850

[21] USAF CROWS Systems Security Engineering Cyber Guidebook, Version 3.0, 2020, http://acqnotes.com/wp-content/uploads/2020/12/SSE-Cyber-Guidebook-v3.0-5-Nov-2020.docx

[22] Director, Operational Test and Evaluations, U.S. Department of Defense, "2020 DOT&E Annual Report", 2021, https://www.dote.osd.mil/Portals/97/pub/reports/FY2020/other/2020DOTEAnnualReport.pdf

9. UNIFIED CERTIFICATION

Combine Verification and Validation Activities
DOTMLPF: Doctrine

9.1 KEY POINTS

- Multiple certification activities can be aligned to reduce cost and schedule for the program

- Seek re-use of Verification & Validation (V&V) events – can a cybersecurity test apply to a nuclear surety certification?

9.2 CASE STUDY

The GBSD program Unified Certification Strategy (UCS)[23] is a multi-level phased certification approach to increase streamlined processes and drive down certification risk grounded in System Theoretic Process Analysis (STPA-Sec) – See paragraph 8. Specific lines of effort include:

Tailored certification policy - GBSD is bringing together certifying authorities within cybersecurity, nuclear surety, and nuclear safety to identify common processes. The goal is to take credit for certification activities from one discipline towards the similar needs of another.

Minimizing size/complexity of the weapon system - GBSD's acquisition strategy[24] is that "a low risk, technically mature baseline design reduces cost/schedule risk by not chasing unproven technology." This approach reduces the chances that yet unproven technologies, requiring more extensive certification efforts, are introduced into the system.

Early identification of certification risks - Regular working groups began after Milestone A in order to bring these security disciplines together to identify risks to timely certification.

Development of tools to enable certification efficiencies - The GBSD program invested significantly in Model Based Systems Engineering (MBSE). By capturing the design of the weapon system digitally, the program can execute certification activities within the model as well. This enables multiple certifying authorities to share artifacts from an authoritative source of truth. Additionally, the GBSD program developed an MBSE profile for cybersecurity, nuclear surety, and nuclear safety. This profile drives the prime contractor to submit artifacts in such a way that the program office can use common tools to analyze the design.

[23] "Ground Based Strategic Deterrent (GBSD) Approach to Defending the Mission", 2021
[24] Col. Jason Bartolomei, "Ground Based Strategic Deterrent (GBSD) Program Overview", 2021

10. MISSION-BASED CYBER RISK ASSESSMENTS (MBCRA)

Continuous mission-focused risk analysis of the weapon system focused on both requirements V&V and vulnerability discovery
DOTMLPF: Materiel

10.1 KEY POINTS

- Continuous analysis of the weapon system starting in Technology Maturation and Risk Reduction (TMRR), executed by the program office, Combined Test Force (CTF) consisting of the Lead Developmental Test Organization (LDTO) and Operational Test Agent (OTA), prime contractor, operational users and defenders, cybersecurity experts, and certification team

- Analysis includes both cooperative and adversarial perspectives, integrating physics-based "art-of-the-possible" and threat intelligence-driven analyses; semi-annual attack path exercises bring stakeholders together to drive data collection and reporting

- Efficient – One combined assessment activity; multiple independent assessments

- Centralized cyberspace picture
  - Informs design, program decisions, follow-on cybersecurity T&E, and other analyses (e.g. STPA-Sec)
  - MBCRAs are updated based on results from hands-on cybersecurity T&E events, intelligence threat analysis, STPA-Sec, or other vulnerability assessment activities

10.2 CASE STUDY

The GBSD MBCRA activities started upon delivery of the preliminary design from the prime contractor prior to Milestone B in Spring 2020, and have been active since then leveraging the USAF Mission Risk Assessment Process for Cyber (MRAP-C) methodology. MBCRA #1 included initial cybersecurity requirements analysis, attack surface characterization, functional thread analysis, attack path vignette development, risk assessment, recommendations for mitigation, and follow on testing / test resources.

Recommendations from MBCRA #1 informed the GBSD EMD Baseline Review (EBR) event and the updated design, which was then evaluated in MBCRA #2 in December 2020. In addition to the core GBSD cybersecurity team (CTF, NG, and SPO), representatives from the 341 Communications Squadron MMIII Mission Defense Team (MDT) and the 346 TS (cybersecurity SMEs) participated in the 2-week exercise. MBCRA #2 included evaluation of approximately 20 attack path vignettes (scenarios) and results informed the program's post-EBR baseline.

Recommendations from MBCRA #2, combined with the updated system design from NG, drove planning for MBCRA #3, which took place in June 2021. This event saw increased participation from core and external stakeholders, and analysis results from this event are driving planning for GBSD's first Cooperative Vulnerability Identification (CVI) test events.

Moving forward, MBCRA analysis will continue at regular intervals, anchored by semi-annual attack path exercises (cybersecurity table-top activities) that bring together external team members and initiate reporting updates. MBCRAs are directing information cybersecurity requirements allocation and derivation at lower levels of the weapon system design as well as aiding in identifying any requirements gaps (requirements validation). MBCRAs are helping drive cyber-related intelligence collection requirements, including but not limited to CIPs. MBCRA scope and results, which are focused on the GBSD WS, are integrated with other program assessment activities to ensure there are no assessment coverage gaps for adversaries to exploit.

APPENDIX A. REFERENCES

[1] Patch, Cully, Cyber Security & Information Systems Information Analysis Center (CSIAC), Personal Correspondence, 24 November 2020.

[2] DOT&E, Cybersecurity Test and Evaluation Guidebook, 10 February 2020, https://www.dau.edu/cop/test/DAU%20Sponsored%20Documents/Cybersecurity-Test-and-Evaluation-Guidebook-Version2-change-1.pdf

[3] Joint Staff, Cyber Survivability Endorsement Implementation Guide, 2019

[4] USAF CROWS Systems Security Engineering Cyber Guidebook, Version 3.0, 2020, http://acqnotes.com/wp-content/uploads/2020/12/SSE-Cyber-Guidebook-v3.0-5-Nov-2020.docx

[5] OUSD R&E, "DoD Instruction 8510.01", 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

[6] Director of Defense R&E, DoD University Affiliated Research Centers (UARC) Management Plan, 2010, https://rt.cto.mil/wp-content/uploads/2019/09/UARC-Mgmt-Plan-Jun-23-10-FINAL-6811-with-Signed-Memo.pdf

[7] MITRE, "FFRDCs—A Primer: Federally Funded Research and Development Centers in the 21st Century", 2015, https://www.mitre.org/sites/default/files/publications/ffrdc-primer-april-2015.pdf

[8] Andrew Rodriguez and David Sawyer, "GBSD Mission Defense & Intel", 2020

[9] OUSD R&E, "DoD Instruction 5000.83", 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf

[10] Northrop Grumman, GBSD, https://www.northropgrumman.com/gbsd/

[11] Exabeam, "Study Reveals 62% of Blue Teams Struggle to Catch Red Teams in Adversary Simulation Exercises", 2020, https://www.exabeam.com/newsroom/study-reveals-62-of-blue-teams-struggle-to-catch-red-teams-in-adversary-simulation-exercises/

[12] Rachel Cohen, "DOD's Cyber 'Red Teams' Stressed as Security Tests Grow," Air Force Magazine, 2019, https://www.airforcemag.com/dods-cyber-red-teams-stressed-as-security-tests-grow/

[13] Director, Operational Test and Evaluations, U.S. Department of Defense, "2020 DOT&E Annual Report", 2021, https://www.dote.osd.mil/Portals/97/pub/reports/FY2020/other/2020DOTEAnnualReport.pdf

[14] David Vergun, "Recruiting Cyber Workforce Easier Than Retaining Them", U.S. Department of Defense News, 2019, https://www.defense.gov/Explore/News/Article/Article/1955580/recruiting-cyber-workforce-easier-than-retaining-them/

[15] John Thomas, "Systems Theoretic Process Analysis (STPA)", 2014, http://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Systems-Theoretic-Process-Analysis-STPA-v9-v2-san.pdf

[16] John Thomas and Matt Gibson, "Industry Trials to Evaluate STPA's Effectiveness and Practicality for Digital Control Systems", 2020, http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/Industry-Trials-to-Evaluate-STPA%E2%80%99s-Effectiveness-and-Practicality.pdf

[17] Tom Leighton, "Technology CEOs Share Best Practices with U.S. Government CIOs", LinkedIn, 2017, https://www.linkedin.com/pulse/technology-ceos-share-best-practices-us-government-cios-tom-leighton-1/

[18] IT Alliance for Public Sector, "Tech Industry's Recommendations for Federal IT Modernization," https://www.itic.org/dotAsset/aa5f716a-2fda-474a-95be-c6778f3783a3.pdf

[19] William Young, "STPA-Sec-Tutorial", 2020, http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/STPA-Sec-Tutorial.pdf

[20] Ivo Friedberg, Kieran McLaughlin, Paul Smith, David Laverty, Sakir Sezer, “STPA-SafeSec: Safety and Security Analysis for Cyber-Physical Systems”, Journal of Information Security and Applications (2016), doi: 10.1016/j.jisa.2016.05.008, 2017, https://www.sciencedirect.com/science/article/pii/S2214212616300850

[21] USAF CROWS Systems Security Engineering Cyber Guidebook, Version 3.0, 2020, http://acqnotes.com/wp-content/uploads/2020/12/SSE-Cyber-Guidebook-v3.0-5-Nov-2020.docx

[22] Director, Operational Test and Evaluations, U.S. Department of Defense, “2020 DOT&E Annual Report”, 2021, https://www.dote.osd.mil/Portals/97/pub/reports/FY2020/other/2020DOTEAnnualReport.pdf

[23] “Ground Based Strategic Deterrent (GBSD) Approach to Defending the Mission”, 2021

[24] Col. Jason Bartolomei, “Ground Based Strategic Deterrent (GBSD) Program Overview”, 2021