CROWS

CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS

Department of the Air Force
Systems Security Engineering Cyber Guidebook

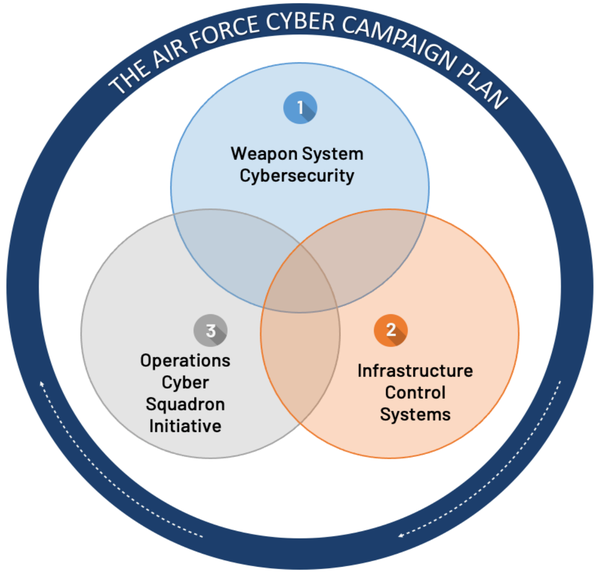
Katie Whatmore, ASB Chief

Cyber Resiliency Office for Weapon Systems

CROWS@US.AF.MIL

A Brief **History** of CROWS

"The task force will **diagnose the extent of the cyber threat and the vulnerabilities** that currently impact our core missions, will plan to develop a risk management plan that will allow the Air Force to fly, fight and win in a cyber-contested environment, and **will recommend investment priorities to the SECAF and CSAF** for how best to address the cybersecurity challenges. - Lt Gen Bill Bender, USAF CIO, 2015

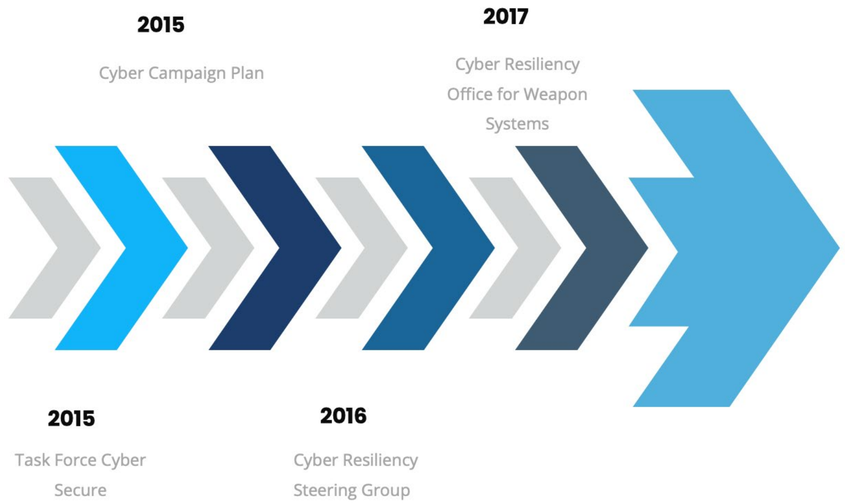


Cyber Campaign Plan

Forged out of 2015's Task Force Cyber Secure, an initiative enacted by then Air Force Chief of Staff Gen. Mark A. Welsh, the Cyber Campaign Plan was developed to synchronize cyber security efforts across the Air Force enterprise to improve the security of information and warfighting systems.

- Acquisition – Weapon System Cyber Resiliency led by the Secretary of the Air Force for Acquisition, Technology, and Logistics (SAF/AQ)
- Infrastructure – Industrial Control Systems and Supervisory Control and Data Acquisition (ICS/SCADA)
- Operations – Communication Squadron Initiative led by the SAF/Chief Information Officer

CROWS TIMELINE

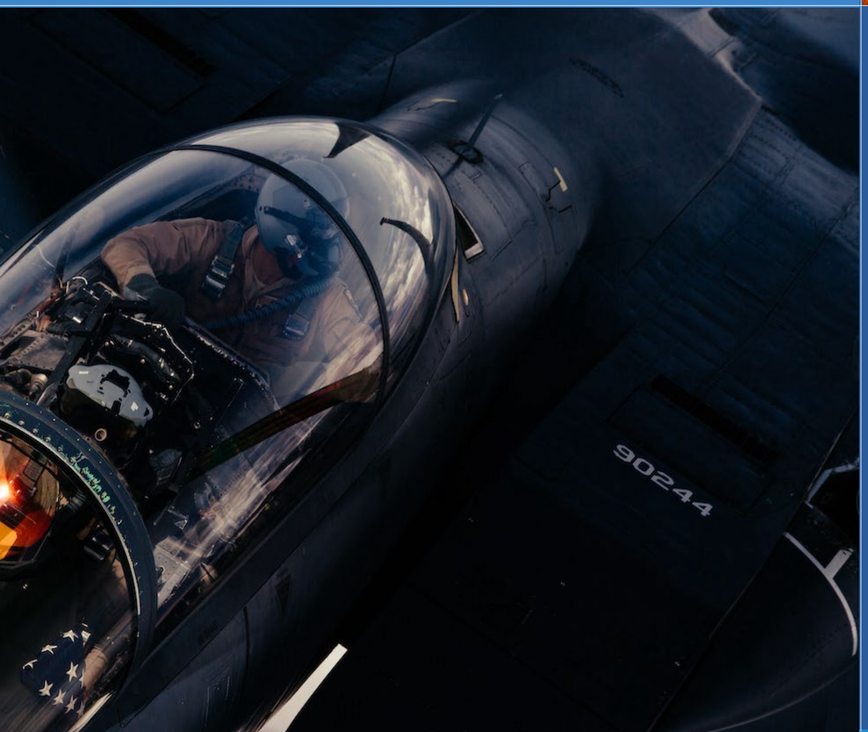


MISSION

INCREASE THE CYBER RESILIENCY OF AIR AND SPACE FORCE WEAPON SYSTEMS TO MAINTAIN MISSION EFFECTIVE CAPABILITY UNDER ADVERSE CONDITIONS

GOALS

BAKE CYBER RESILIENCY INTO NEW WEAPON SYSTEMS AND MITIGATE CRITICAL VULNERABILITIES IN FIELDED WEAPON SYSTEMS



VISION

CYBER RESILIENCY EMBEDDED INTO AIR AND SPACE FORCE WEAPON SYSTEMS AND INGRAINED IN DEPARTMENT OF THE AIR FORCE CULTURE

Systems Security Engineering

Policy and Guidance

Current policy is diverse and comes from many governing authorities

These policies are executed through PP and SSE

SYSTEM SECURITY ENGINEERING

CPI/CPTI/AT

Policy:
- DoDI 5200.FH
- DoDI 5200.39
- DoDM 5200.45
- DoDI 5200.48
- DoDD 5200.47E
- DoDM 5200.01
- USD (R&E) Memo

Cyber Resiliency

Guidance:
- JCIDS CSEIG
- JCIDS Manual

Standards:
- NIST SP800-34
- NIST SP800-160

Cybersecurity

Law:
- E.O. 14028
- E.O. 13694

Policy:
- DoDI 5000.02
- DoDI 5000.90
- DoDI 8500.01
- DoDI 8510.01
- AFI 17-101
- AFI 17-130

Standards:
- NIST SP800-53
- NIST SP800-171

Security Management

Law:
- DoDM 5205.07, V1-V4
- DoDI 5200.48
- DoDM 5200.1, V1-V3
- DoDM 5220.22, V2
- DoDM 5200.2
- DoDM 5205.02
- DoDI 5200.48
- AFMAN 16-1404, V1-V3
- DAFMAN 16-703, V1
- AFMAN 16-703, V3

TSN

Policy:
- DoDI 5200.44
- AFMC TSN Implementation Plan

ZTA

Guidance:
- DoD Zero Trust Reference Architecture

TEST & EVALUATION

Policy

10 U.S.C. 2399 | DoDI 5000.02 | DoDI 8500.01 | DoDI 8510.01 | AFI 99-103 | AFMAN 63-119

Guidance

DoD Cybersecurity Test & Evaluation Guidebook | JCIDS Cyber Survivability Endorsement Implementation Guide

PROGRAM PROTECTION

Policy

10 U.S.C. 2224 | DoDI 5000.02 | DoDI 5000.83 | DoDD 5240.1 | AFI 63-101/20-101 | DAFI 63-113

AFLCMC Official Memorandum on Technology/Acquisition Program Protection

Guidance

Department of the Air Force System Security Engineering Cyber Guidebook

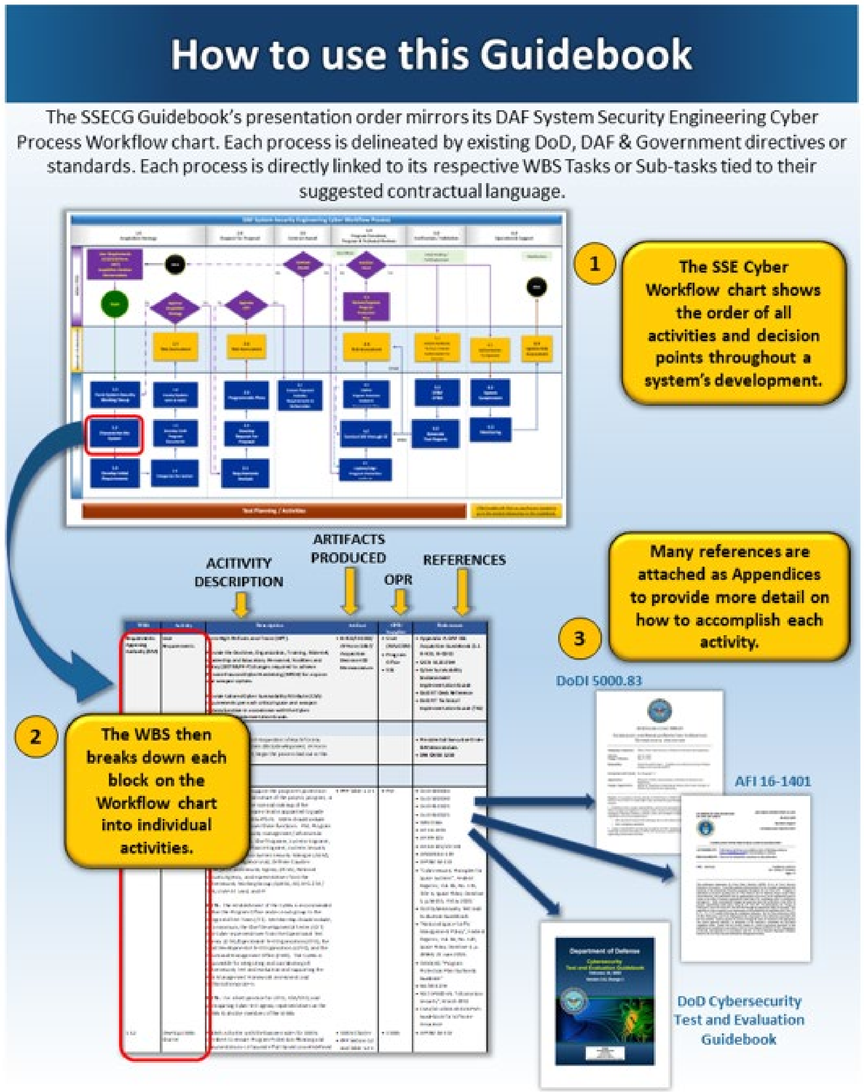
OPERATIONAL RESILIENCY

Manual

AFM 1-1 V1-V2 | AFDP-1

Take-away:
Through the SSECG, the ASB is trying to help you "work smarter, not harder"

SSECG V5.0 Summary

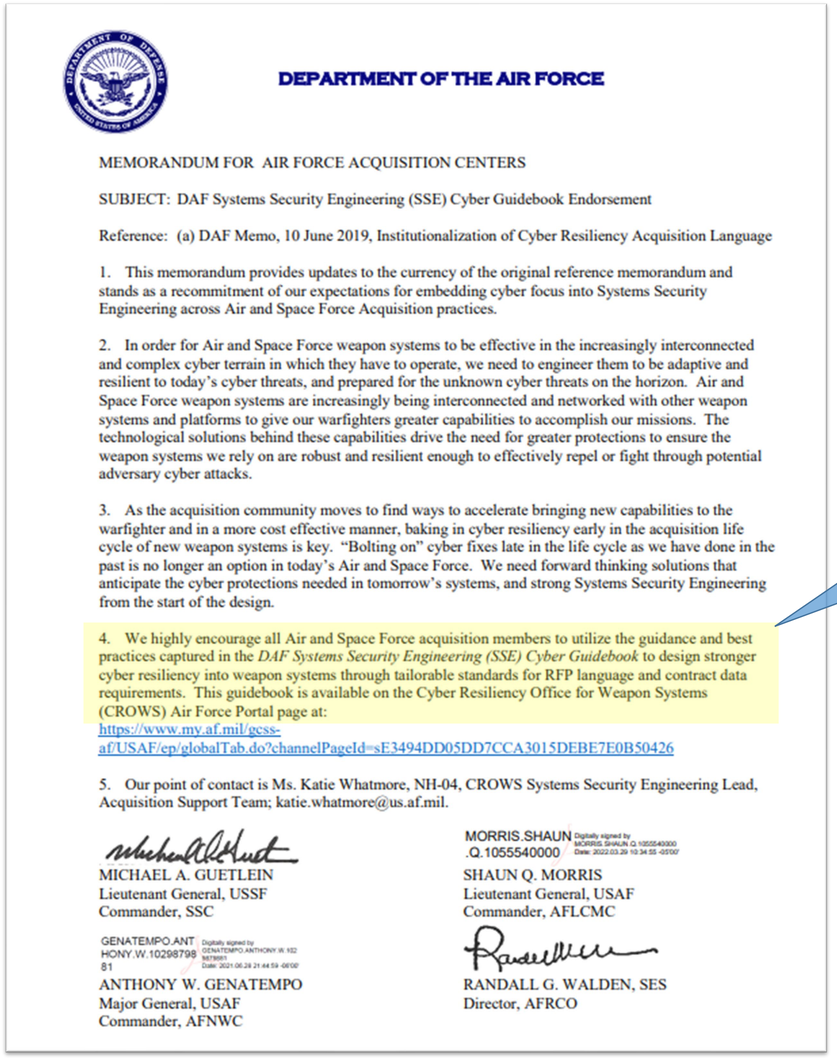


Content

- Main Body- SSE Cyber Process Guidebook
  - Executive Summary
  - Detailed Work Breakdown Structure in Section 4
  - Includes figures in Section 4 to help users link the SSE Workflow Process to the Acquisition Life Cycle phases
- Supplemental Appendices
  - Appendix A: DAF SSE Acquisition Guidebook
  - Appendix B: DAF Combined Process Guide for CPI/CC Identification
  - Appendix C: Functional Thread Analysis
  - Appendix D: Attack Path Analysis
  - Appendix E: Design Considerations
  - Appendix F: Relationship to Other Processes
  - Appendix G-J: Definitions, Acronyms, References, and Templates

Note: V5 is currently Distro D and still undergoing public release review

Memorandum & Endorsement



DEPARTMENT OF THE AIR FORCE

MEMORANDUM FOR AIR FORCE ACQUISITION CENTERS

SUBJECT: DAF Systems Security Engineering (SSE) Cyber Guidebook Endorsement

Reference: (a) DAF Memo, 10 June 2019, Institutionalization of Cyber Resiliency Acquisition Language

1. This memorandum provides updates to the currency of the original reference memorandum and stands as a recommitment of our expectations for embedding cyber focus into Systems Security Engineering across Air and Space Force Acquisition practices.

2. In order for Air and Space Force weapon systems to be effective in the increasingly interconnected and complex cyber terrain in which they have to operate, we need to engineer them to be adaptive and resilient to today's cyber threats, and prepared for the unknown cyber threats on the horizon. Air and Space Force weapon systems are increasingly being interconnected and networked with other weapon systems and platforms to give our warfighters greater capabilities to accomplish our missions. The technological solutions behind these capabilities drive the need for greater protections to ensure the weapon systems we rely on are robust and resilient enough to effectively repel or fight through potential adversary cyber attacks.

3. As the acquisition community moves to find ways to accelerate bringing new capabilities to the warfighter and in a more cost effective manner, baking in cyber resiliency early in the acquisition life cycle of new weapon systems is key. "Bolting on" cyber fixes late in the life cycle as we have done in the past is no longer an option in today's Air and Space Force. We need forward thinking solutions that anticipate the cyber protections needed in tomorrow's systems, and strong Systems Security Engineering from the start of the design.

4. We highly encourage all Air and Space Force acquisition members to utilize the guidance and best practices captured in the *DAF Systems Security Engineering (SSE) Cyber Guidebook* to design stronger cyber resiliency into weapon systems through tailorable standards for RFP language and contract data requirements. This guidebook is available on the Cyber Resiliency Office for Weapon Systems (CROWS) Air Force Portal page at:
https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=sE3494DD05DD7CCA3015DEBE7E0B50426

5. Our point of contact is Ms. Katie Whatmore, NH-04, CROWS Systems Security Engineering Lead, Acquisition Support Team; katie.whatmore@us.af.mil.

MICHAEL A. GUETLEIN
Lieutenant General, USSF
Commander, SSC

MORRIS.SHAUN.Q.1055540000 Digitally signed by MORRIS.SHAUN.Q.1055540000 Date: 2022.03.29 10:34:55 -05'00'
SHAUN Q. MORRIS
Lieutenant General, USAF
Commander, AFLCMC

GENATEMPO.ANTHONY.W.1029879881 Digitally signed by GENATEMPO.ANTHONY.W.1029879881 Date: 2021.06.28 21:44:59 -04'00'
ANTHONY W. GENATEMPO
Major General, USAF
Commander, AFNWC

RANDALL G. WALDEN, SES
Director, AFRCO

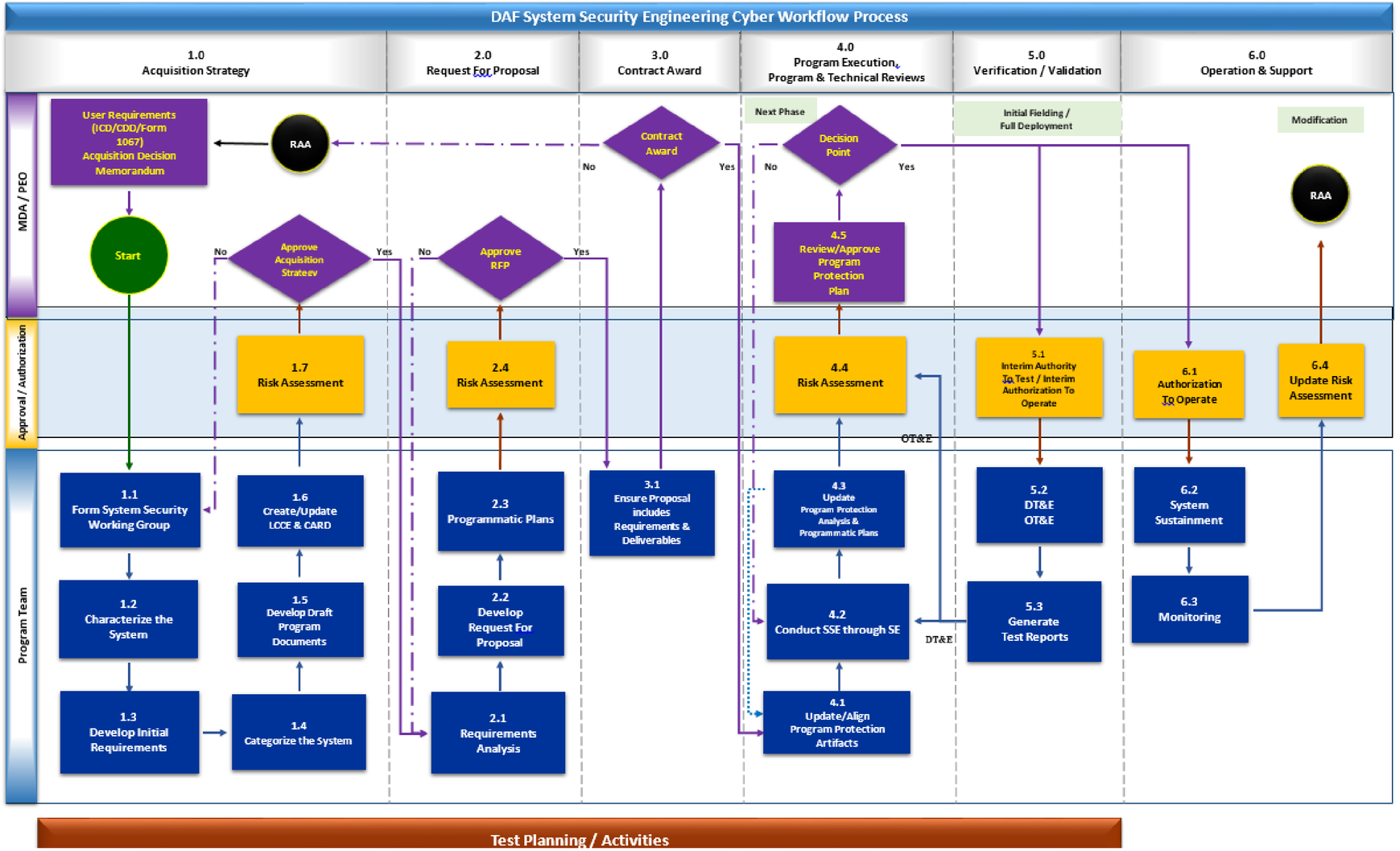
4. We highly encourage all Air and Space Force acquisition members to utilize the guidance and best practices captured in the DAF Systems Security Engineering (SSE) Cyber Guidebook to design stronger cyber resiliency into weapon systems through tailorable standards for RFP language and contract data requirements.

The need for this guidebook and its contents has been endorsed by the following organizations:

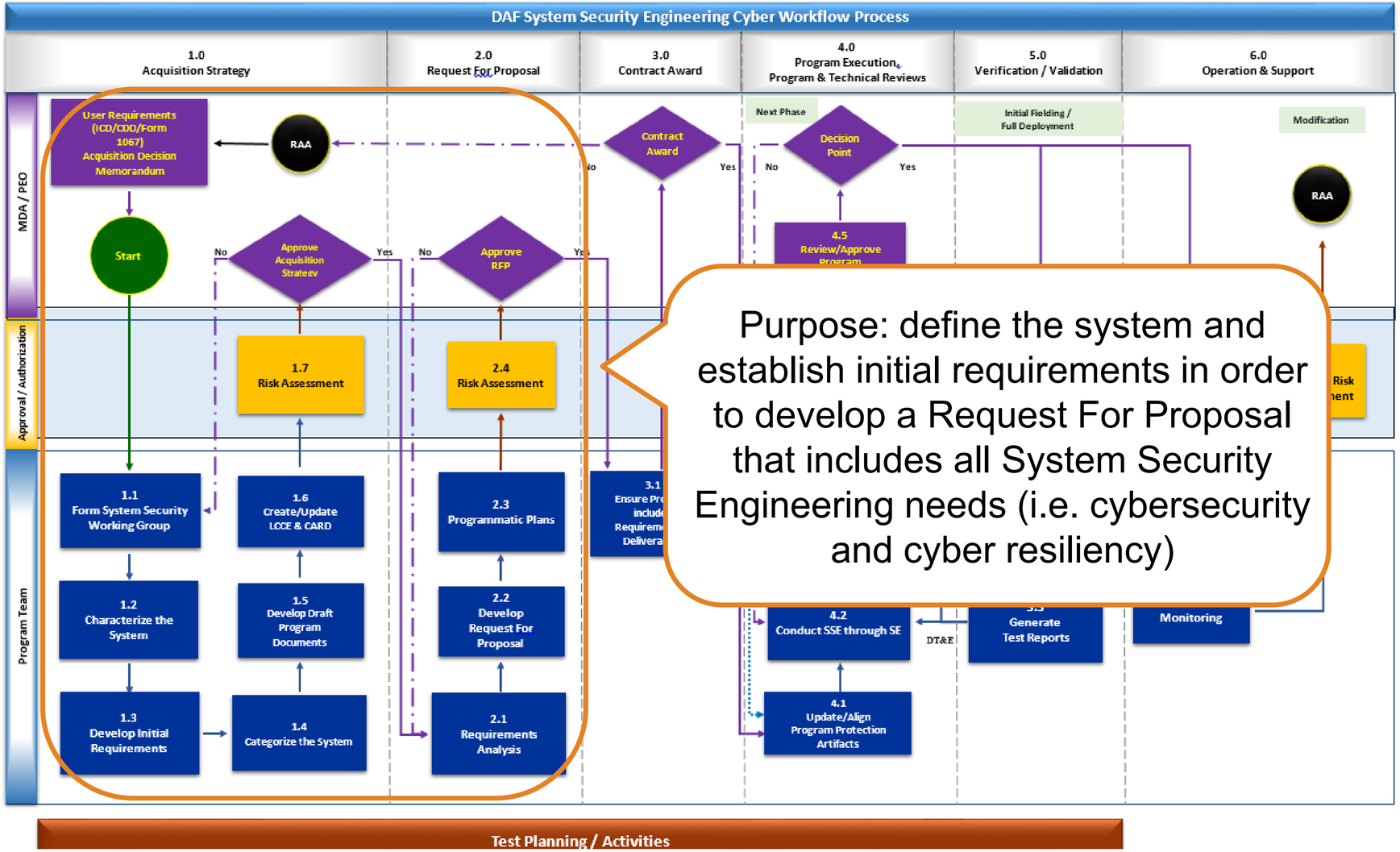
- **United States Air Force Life Cycle Management Center**
- **United States Air Force Space and Missile Systems Center**
- **United States Air Force Nuclear Weapons Center**
- **United States Air Force Rapid Capabilities Office**
- **Naval Air Systems Command (NAVAIR) Cyber Warfare Department**
- **National Defense Industrial Association (NDIA) Systems Security Engineering Committee**

National Defense Industrial Association

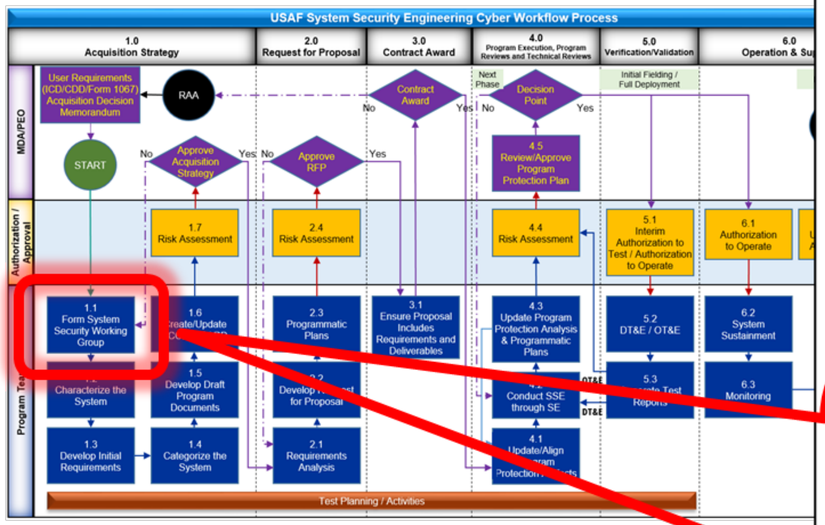
DAF SSE Cyber Workflow Process



DAF SSE Cyber Workflow Process



DAF SSE Cyber Workflow Process



The WBS provides a complete description of each activity identified in the Workflow Process

Table 4-1 Work Breakdown Structure (WBS) for the SSE Cyber Workflow Process

WBS	Activity	Description	Artifact	OPR/ Supplier	References
Requirements Approving Authority (RAA)	User Requirements	Form High Performance Team (HPT). Provide tailored Cyber Survivability Attribute (CSA) requirements per each critical weapon system function in accordance with the Cyber Survivability Implementation Guide.	• ICD/CDD/ AF Form 1067/ Acquisition Decision Memorandum	• User (MAJCOM) • Program Office • SSE	• Appendix A: USAF SSE Acquisition Guidebook (1.1 ICD, CDD) • Cyber Survivability Endorsement Implementation Guide • DoD AT Desk Reference • DoD AT Technical Implementation Guide (TIG)
1.0	**Acquisition Strategy**				
START	Enter DoD Acquisition Life Cycle	Upon entering the DoD Acquisition Life Cycle for any weapon system development, AF Form 1067 or new contract, begin the process laid out			
1.1	**Form Systems Security Working Group (SSWG)**				
1.1.1	Appoint Personnel to SSWG / appropriate IPT	Assemble a team to support the program's protection planning. The size and nature of the project, program, or system will dictate the size and makeup of the protection team. Ensure a lead is appointed to guide and facilitate the SSWG efforts SSWG should include personnel that can cover these functions PM, program protection lead (security management/ information protection), logistics, chief engineer, systems engineer, systems security engineer, information system security manager (ISSM), intelligence, Defense CounterNASIC and Security Agency (DCSA), National Security Agency, and representatives from the Cybersecurity Working Group (CyWG), AO, TSN, USAF AT Lead, and IP. NOTE: The establishment of the CyWG is recommended within the Program Office, and as a sub-group to the Integrated Test Team (ITT). Membership should include, as a minimum, the Chief Developmental Tester (CDT) and cyber representatives from the Operational Test	• PPP Table 1.2-1	• PM	• DoDI 8510.01 • DoDI 5000.02T • DoDI 8500.01 • AFI 99-103 • AFMAN 63-119 • AFPAM 63-113 • Appendix B: USAF Combined Process Guide for CPI and CC Identification • OSD PPP Outline & Guidance

DAF SSECG Appendix A Summary

SSE in Request For Proposal (RFP)

- SOO/SOW Language (tailorable)
- CDRLs with corresponding DIDs that are mapped to the SOO/SOW paragraphs
- SRD (148 tailorable system level requirements)
- Recommended FAR/DFARS/AFFARS
- Section L language
- Section M language
- Systems Engineering Technical Review Entrance Criteria
  - ASR, SR, SFR, PDR, CDR, FCA, SVR, PRR, PCA

SSE in Programmatic Documents

- Program Protection Plan (PPP)
- Information Support Plan (ISP)
- Systems Engineering Plan (SEP)
- Life Cycle Sustainment Plan (LCSP)
- Test and Evaluation Master Plan (TEMP)
- Life-Cycle Cost Estimate (LCCE)
- Cost Analysis Requirements Description (CARD)

10

DAF SSECG Appendix A

SSE in Request For Proposal (RFP)

- SOO/SOW Language (tailorable)
- CDRLs with corresponding DIDs that are mapped to the SOO/SOW paragraphs
- SRD (148 tailorable system level requirements)
- Recommended FAR/DFARS/AFFARS
- Section L language
- Section M language
- Systems Engineering Technical Review Entrance Criteria
  - ASR, SR, SFR, PDR, CDR, FCA, SVR, PRR, PCA

Appendix A: SSE Acquisition Guidebook

2.0 Requirements Documents

2.3 Statement of Objectives and Statement of Work

2.3.2. Program Protection

A. The contractor shall deliver a Program Protection Implementation Plan (PPIP), CDRL 1, that is aligned to the Government developed Program Protection Plan (PPP). The contractor shall integrate the PPIP activities in the Integrated Master Plan/Integrated Master Schedule (IMP/IMS) (CDRL 10).

B. The Contractor shall create, maintain and operate a formal incident response and forensic capability for protection of Control Unclassified Information (CUI) residing on non-federal Information Systems. The Contractor shall include the subcontractors and suppliers that perform support work that involves CUI. The scope and extent of this incident response and forensic capability shall be consistent with the assigned Contractor's Cyber Maturity Model Certification (CMMC) level (CDRL TBD).

C. The Contractor shall establish a System Security Plan (SSP) citing Cyber Incident Reporting (IR) requirements. Any IR that impacts a Contractor system under the contract's DFAR clauses and provisions must be reported within 72 hours of the suspected incident. To report cyber incidents, the Contractor must have a medium assurance certificate. A review must be conducted so that the scope of the compromise can be understood. At a minimum, this review must cover the information specified in DID xx and as cited in CDRL 19 and under NIST SP800-61 Rev. 2 guidelines. As a minimum, the CDRL 19 must provide IR review reporting to include, but not limited to: Identification of affected systems; Affected Users accounts; Affected data; and Other systems that might have been compromised.(CDRL 19)

D. The Contactor shall be prepared and report cyber incidents that result in an actual or potentially

11

DAF SSECG Appendix A

SSE in Request For Proposal (RFP)

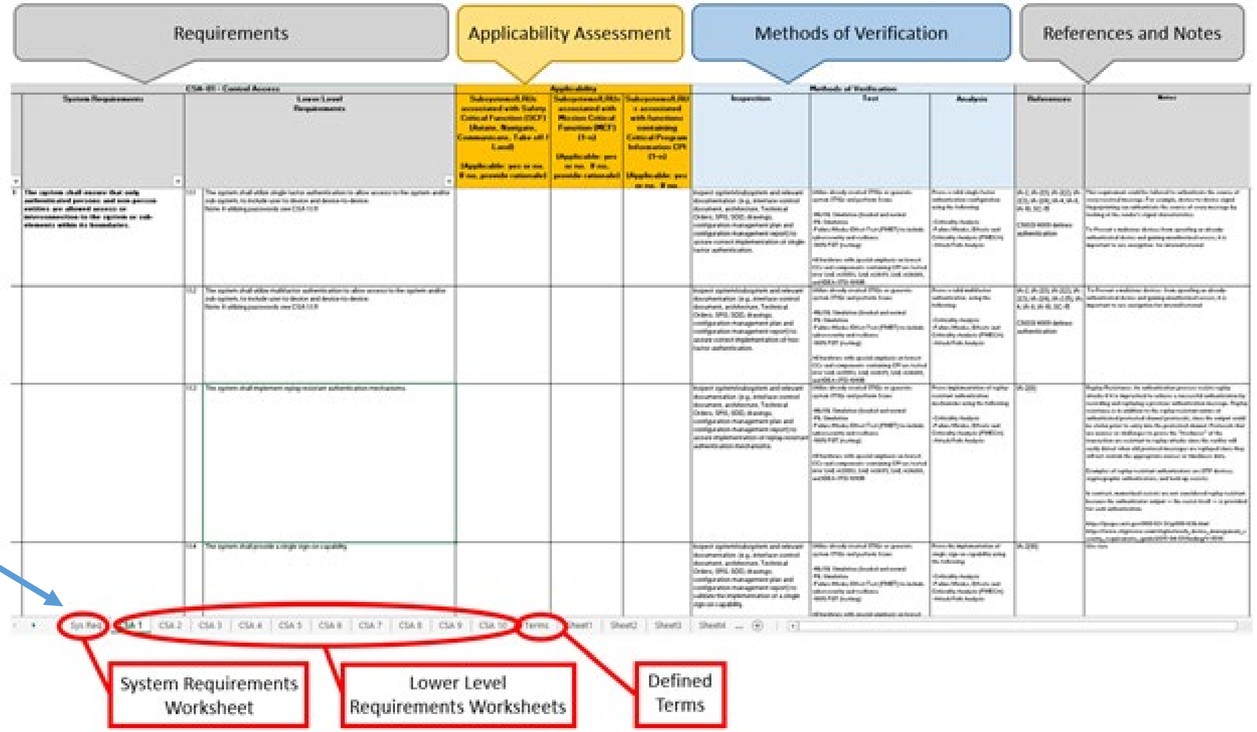
- SOO/SOW Language (tailorable)
- CDRLs with corresponding DIDs that are mapped to the SOO/SOW paragraphs
- SRD (148 tailorable system level requirements)
- Recommended FAR/DFARS/AFFARS
- Section L language
- Section M language
- Systems Engineering Technical Review Entrance Criteria
  - ASR, SR, SFR, PDR, CDR, FCA, SVR, PRR, PCA

Per DD Form 1423-1 Block 7, all CDRLs should specify requirement for inspection/acceptance of the data item by the Government.						
Guidebook Section SOO/SOW Reference	CDRL	Name	Title (DD Form 1423-1, Block 2)	DID (DD Form 1423-1, Block 4)	Recommended Delivery Schedule (DD Form 1423-1, Block 12 and Block 13)	Recommended Remarks (DD Form 1423-1, Block 16)
2.3.2 A	1	Program Protection Implementation Plan (PPIP)	Program Protection Implementation Plan (PPIP)	DI-ADMN-81306	60 Days after contract award Concept Plan 105 days prior to Milestone A Plan 60 days prior to PDR (or 105 days prior to Milestone B, whichever is sooner) Final Plan 60 days prior to CDR Initial AT Evaluation Plan60 days prior to PDR Final V&V Plan 60 days prior to CDR V&V Report 120 days prior to Milestone C Update annually	Follow the newest OSD PPP template
2.3.1 B 2.3.1 C	2	Specification	Program-Unique Specification Documents	DI-SDMP-81493, or DI-IPSC-81431A	Standard program delivery	
2.3.1 B 2.3.1 C	3	Specification	Interface Requirements Specification (IRS)	DI-IPSC-81434	Preliminary draft for each Configuration Item (CI) / Computer Software Configuration Item (CSCI) due 30 days prior to SFR Updates as required	

DAF SSECG Appendix A

SSE in Request For Proposal (RFP)

- SOO/SOW Language (tailorable)
- CDRLs with corresponding DIDs that are mapped to the SOO/SOW paragraphs
- SRD (148 tailorable system level requirements)
- Recommended FAR/DFARS/AFFARS
- Section L language
- Section M language
- Systems Engineering Technical Review Entrance Criteria
  - ASR, SR, SFR, PDR, CDR, FCA, SVR, PRR, PCA



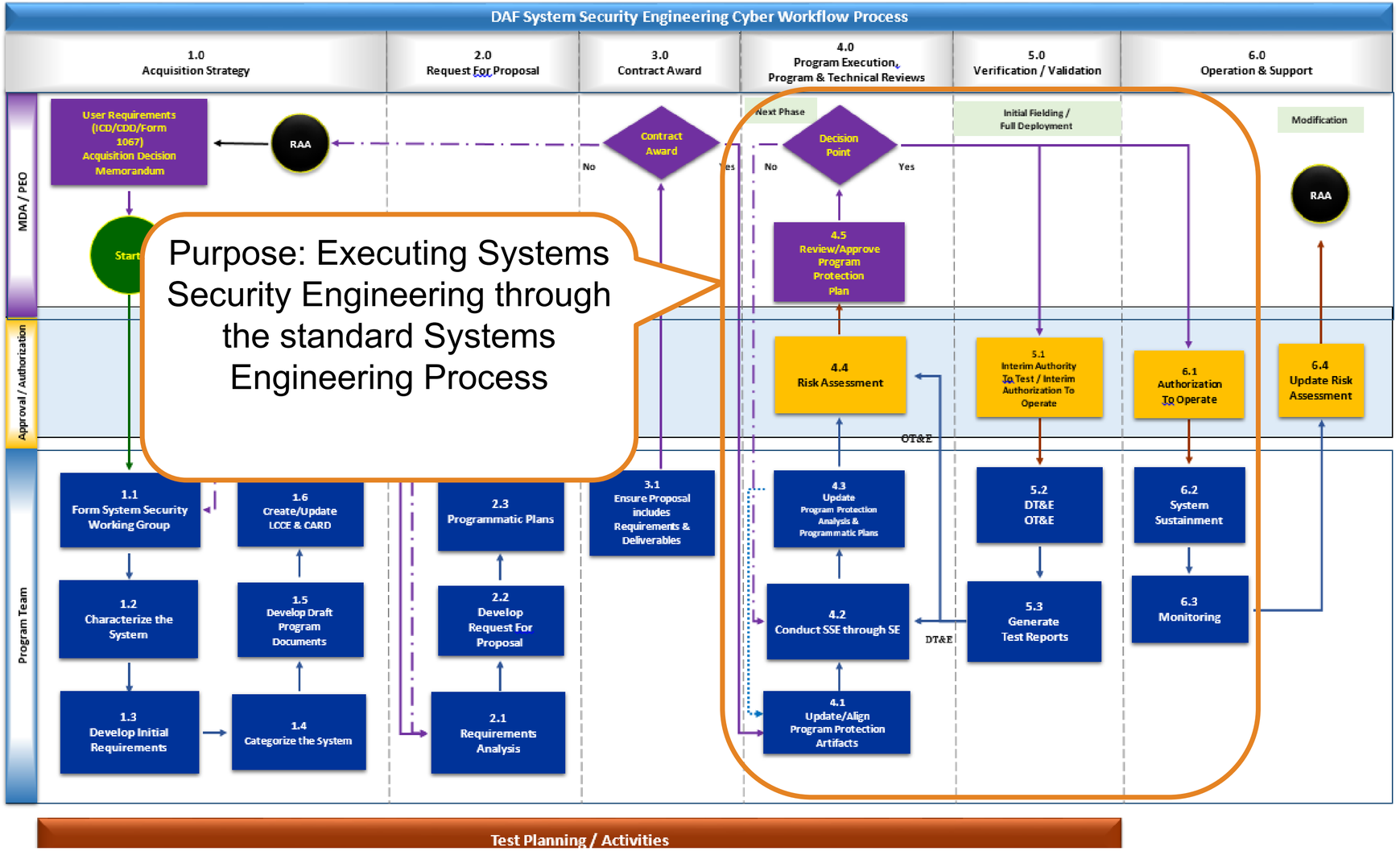
SSECG and Program Protection

- **Section 1**: Introduction – Purpose and Update Plan
- **Section 2**: Program Protection Summary
- **Section 3:** Critical Program Information (CPI) and Critical Components (CC)
- **Section 4:** Horizontal Protection
- **Section 5:** Threats, Vulnerabilities, and Countermeasures
- **Section 6:** Other System Security-Related Plans and Documents
- **Section 7:** Program Protection Risks
- **Section 8:** Foreign Involvement
- **Section 9:** Processes for Management and Implementation of PPP
- **Section 10:** Processes for Monitoring and Reporting Compromises
- **Section 11:** Program Protection Costs
- **Appendix A:** Security Classification Guide
- **Appendix B:** Counterintelligence Support Plan
- **Appendix C**: Criticality Analysis
- **Appendix D:** Anti-Tamper Plan
- **Appendix E:** Cybersecurity Strategy (CSS)

The OSD PPP guide/template: https://www.milsuite.mil/book/servlet/JiveServlet/downloadBody/248833-102-2-441341/PPP-Outline-and-Guidance-v1-July2011.pdf

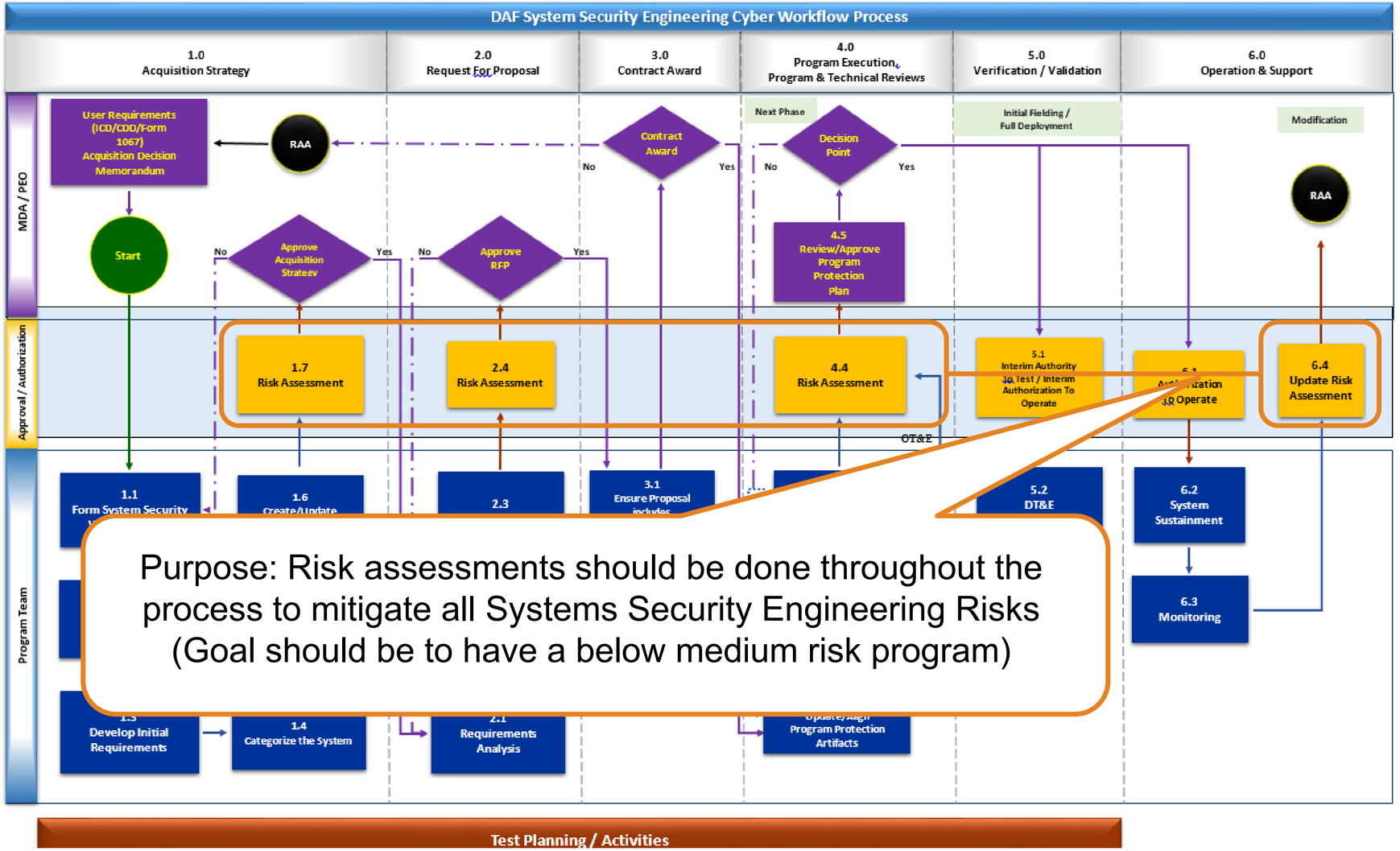
The DAF SSECG helps populate the shaded sections of the PPP

DAF SSE Cyber Workflow Process



15

DAF SSE Cyber Workflow Process

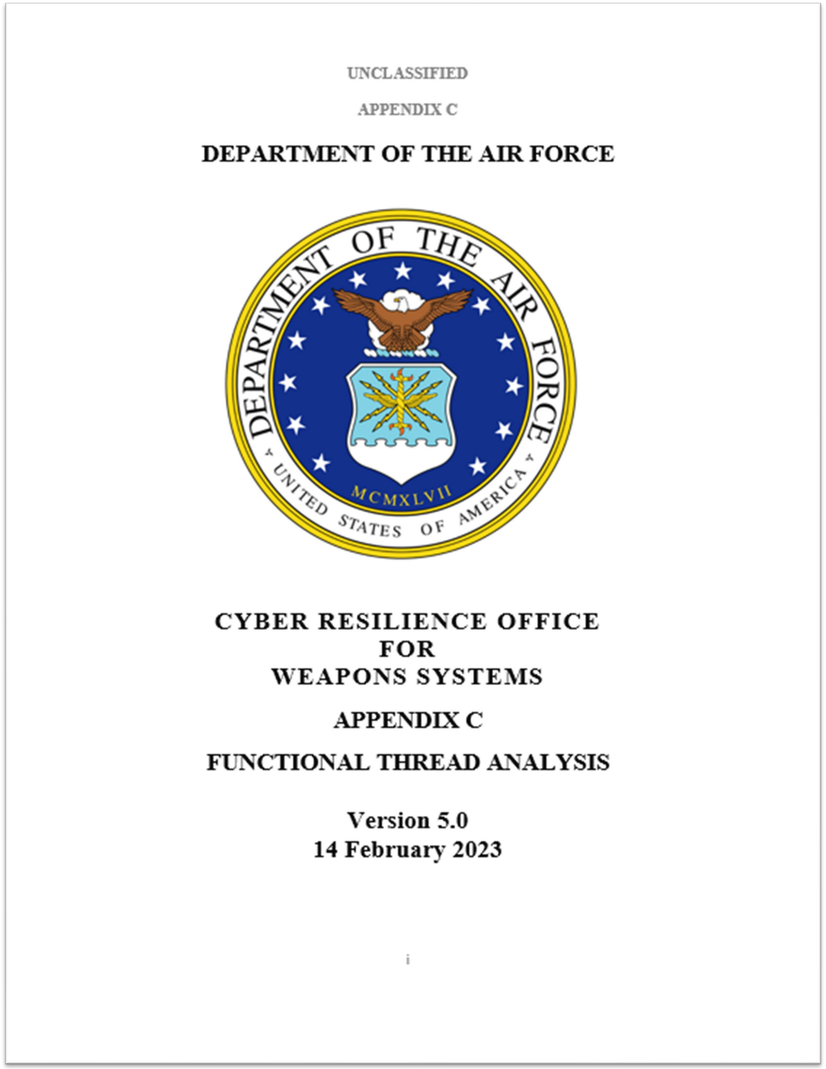


Purpose: Risk assessments should be done throughout the process to mitigate all Systems Security Engineering Risks (Goal should be to have a below medium risk program)

16

DAF SSECG Appendix C Summary

- Functional Thread Analysis (FTA) includes the following activities:
  - Functional Decomposition
  - Entry Access Points Identification
  - Attack Path Vignette Development
- The Functional Thread Analysis provides guidance on how to functionally decompose a system from the mission to the component level.
- The FTA is an iterative process that should be updated in conjunction with a program's Systems Engineering Technical Reviews (SETRs).
- Ultimately, the FTA and Attack Path Analysis (next slide) process will assist programs to establish informed risks.



UNCLASSIFIED

APPENDIX C

DEPARTMENT OF THE AIR FORCE

CYBER RESILIENCE OFFICE
FOR
WEAPONS SYSTEMS

APPENDIX C

FUNCTIONAL THREAD ANALYSIS

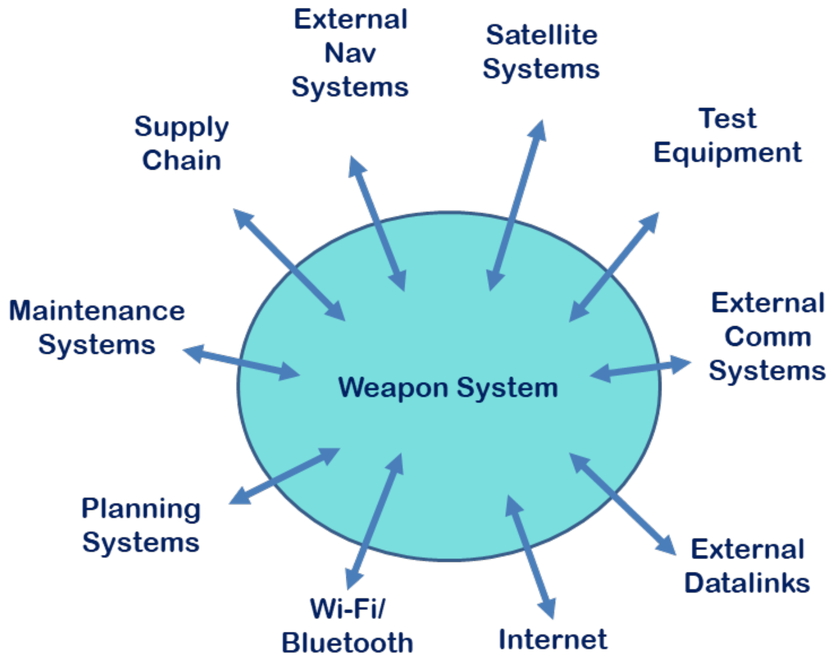
Version 5.0
14 February 2023

i

17

DAF SSECG Appendix D Summary

- FTA (appendix C) is foundation
  - Information
  - Documentation
  - Source Material
- Attack Path Vignettes (APV)
  - Lexicon… the building blocks
  - Generate & combine cyber vulnerabilities into cyber attack scenarios
- Appendix D provides guidance on APA and the following:
  - Attack Path Exercise (APE)
- Primary drivers
  - Milestone
  - SETRs

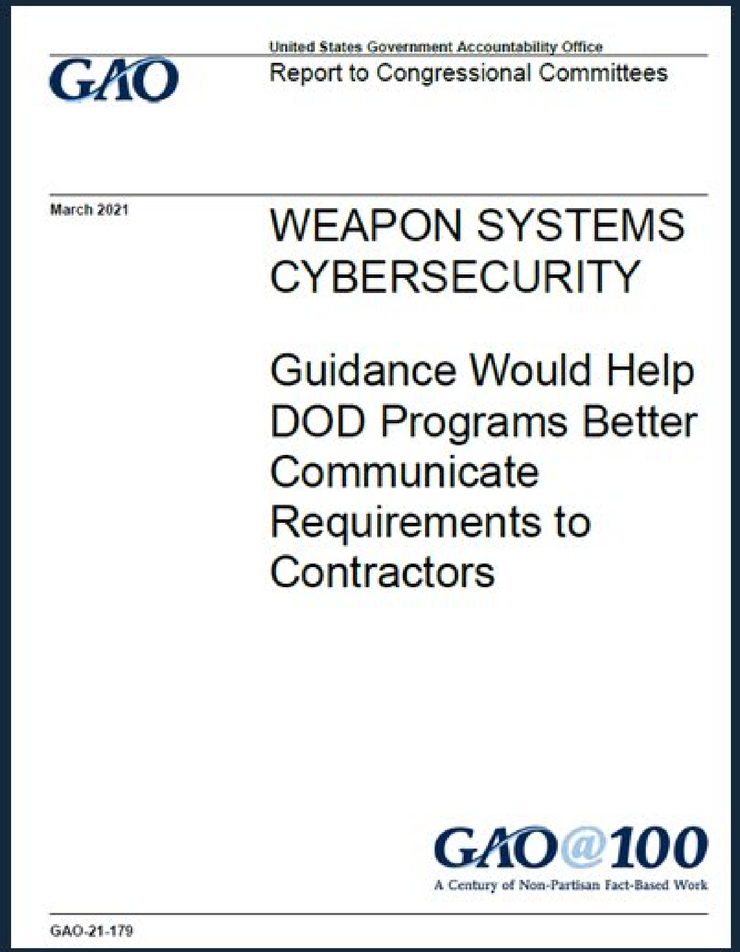


The Attack Path Analysis (APA) focuses on:
- Where the threat (e.g. attacker) can gain access?
- Which paths can be used to attack/exploit the system?
- What are the potential mission effects?

18

QUESTIONS ?

2021 GAO Report on Weapon Systems Cybersecurity



United States Government Accountability Office

GAO

Report to Congressional Committees

March 2021

WEAPON SYSTEMS CYBERSECURITY

Guidance Would Help DOD Programs Better Communicate Requirements to Contractors

GAO@100

A Century of Non-Partisan Fact-Based Work

GAO-21-179

"Current military service guidance, **except for the Air Force**, does not address how acquisition programs should contract for weapon systems cybersecurity requirements, acceptance criteria, and verification, which DOD and program officials told GAO would be helpful."

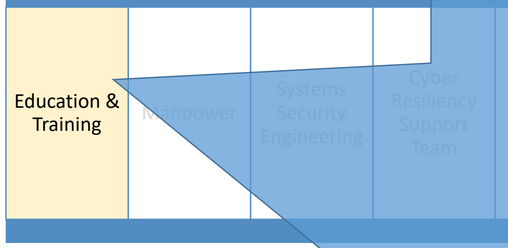
"The **Air Force has recently issued service-wide guidance specific to contracting for cybersecurity**, in part by leveraging existing departmental policies and guidance."

"Among other things, the **CROWS Guidebook provides sample language that programs could include in their requests for proposals, statements of work, and other contract documents**."

"The Air Force has taken positive actions to remedy this by developing internal guidance on how to incorporate program-specific cybersecurity requirements. The Army, Navy, and Marine Corps would benefit from a similar approach."

Education and Training

Acquisition Support Branch



EDUCATION

- Leveraging existing courses and building from scratch
- Cyber Education Consortium: CROWS, DAU, AFIT, AF Cyber College, NAVAIR, ACE
- Implementing “Learning Paths” to take basic engineer or IT professionals and get them cross-certified (i.e., engineers that know IT and IT personnel that know engineering

TRAINING

- The System Security Engineering Cyber Practitioners course is a practitioners-level course that examines, in-depth, the Department of the Air Force (DAF) Systems Security Engineering (SSE) Cyber Guidebook.
- Developed for the experienced Acquisition workforce, the goal of the SSE Practitioners Course is to enable the SSE practitioner to fully apply the SSE Cyber Workflow Process to their program, regardless of where the program is in the acquisition lifecycle.
- 4-day instructor-led course consists of two workshops, A and B, and covers a total of seven modules. The content includes a use case that utilizes the processes included in the SSE Cyber Guidebook and is supplemented by hands-on exercises.
- Some of the topics covered include functional thread analysis, attack path analysis, completion of a risk assessment, and developing contract language. In addition to the subject matter, the workshops integrate the use of additional guidebooks and DOD directives as they apply to addressing cyber during the Systems Security Engineering process.

*Education, Training, & Manpower’s goal is to **change the Air Force acquisition culture** from within through hiring, education, and training, thus providing the right people at the right place with the right systems and tool knowledge*