TRIDIUM talk

MEETING GOVERNMENT CYBERSECURITY REQUIREMENTS WITH THE niagara framework®

WITH SPECIAL
GUEST PRESENTER:

ALETA Technologies

MAY 28, 2020

HOUSEKEEPING

- Questions should be submitted using the Q&A Tab

- This session will be recorded. The recording will be available soon after the sessions ends and will be posted at www.tridium.com/en/resources/events

+ 2020 TridiumTalks

AGENDA

- Team Introduction
- Risk Management Framework (RMF) Overview
- UFC 4-010-06 & UFGS 25 05 11
- Deciphering Government Proposals with RMF Requirements
- Subcontractor Cyber Responsibilities
- Schedule & Cost Impacts

ALETA TEAM - PRESENTER

JAY KUROWSKY

- President & CEO, Aleta Technologies
- 24 years' experience in cyber and Information Security (INFOSEC), including 23 years' experience in leading high-performing cyber and INFOSEC organizations
- Served as an Army Acquisition Corps member, Vice-President of a large, publicly-traded corporation, and technical representative to the Three-star General CIO/G-6 of the Army
- Provided cybersecurity support to over 1,000 systems
- Advised the Pentagon on cybersecurity issues such as malicious content in commercial software and security accreditation
- Served as Army's representative for Software Protection/Anti-tamper
- Experience drafting policy for the Office of the Principal Cyber Advisor to the Secretary of Defense
- Bachelor of Science degree in Mechanical Engineering, Masters' in Management/Information Systems
- Certifications/Awards include CISSP, Black Belt in Lean Six Sigma, three Army medals, and various other awards and commendations

ALETA TEAM - Q&A

HERNDON ELLIOTT

- Senior Cybersecurity Subject Matter Expert, Aleta Technologies
- Prior Army GS-15 with over 30 years of service
- 15 years as CIO of 10,000-person Army Aviation and Missile R&D laboratory, 6 years as Army-appointed validator under DIACAP (ACA) + 2 years appointed as validator under RMF (SCA-V)
- Prior Army Acquisition Corps Member, Level III certified in Systems Planning, Research, Development, and Engineering
- BSCE, Master of Science in Computer Science, CISSP

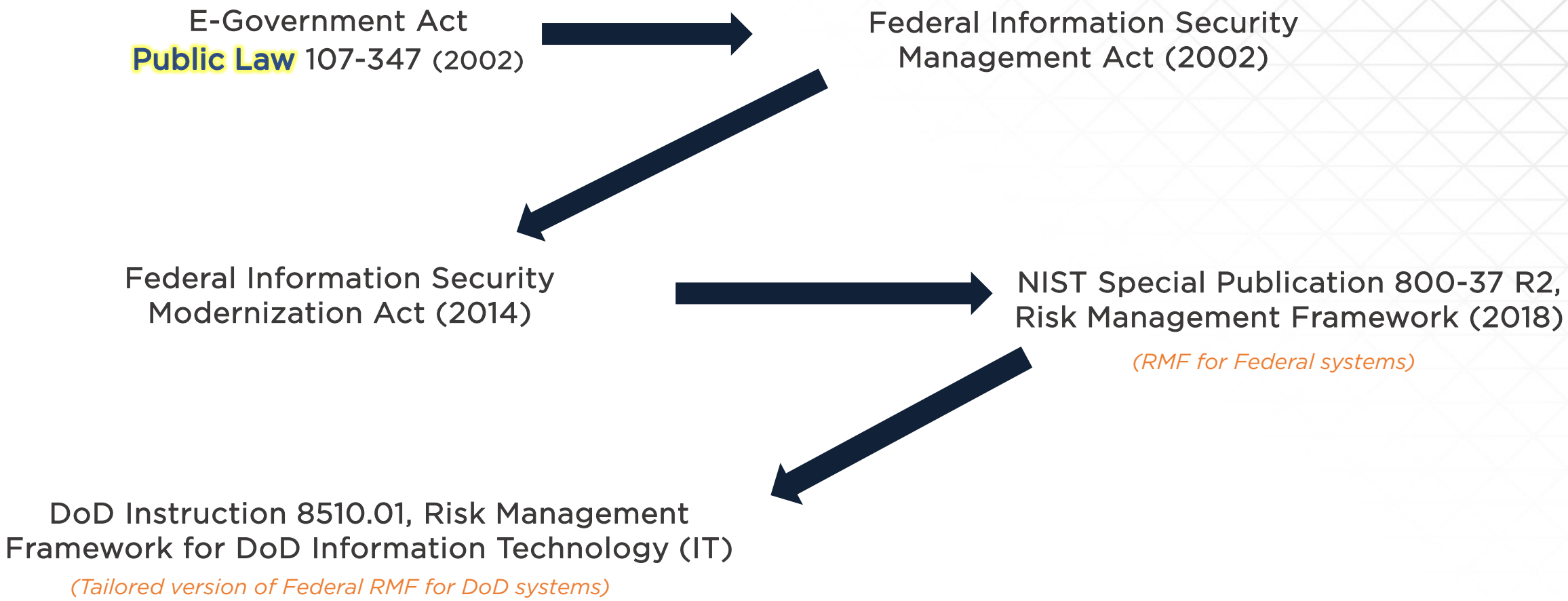
TODD HEFLIN

- Senior Cyber Architect, Aleta Technologies
- Former SCA-V representative, supporting the Gov't third-party assessor
- Skilled in penetration testing, security hardening, and security engineering
- Experience writing cyber policy on behalf of the U.S. Army
- Master of Science, Cybersecurity and Information Assurance
- Global Industrial Cyber Security Professional, CISSP, and Certified Ethical Hacker

NEW ATTENTION FOR CYBERSECURITY

- Cybersecurity requirements for control systems/operational technology have existed for years within the U.S. Department of Defense (DoD) and the broader Federal Government, though these systems have historically gotten less attention than other systems
- Recent events are causing focus on cybersecurity for control systems, and to increasing extent
  - 1 May 2020 Presidential Executive Order, *Securing the United States Bulk Power System*
  - DoD Memorandums, Execution Orders, and Inspector General Audit reports
  - Stuxnet, Havex, and other attacks
  - Risk Management Framework (RMF) is the basis for most requirements

RMF GENESIS



NIST = National Institute of Standards & Technology
DoD = Department of Defense

SECURITY AUTHORIZATION

- The Risk Management Framework (RMF) for DoD Information Technology (IT) is based on National Institute for Standards and Technology (NIST) process
- Per NIST SP 800-37: “Security authorization is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.”
- Per DoD Instruction 8510.01 (“the RMF”): “This instruction applies to:… All DoD IT that receive, process, store, display, or transmit DoD information. These technologies are broadly grouped as DoD IS, platform IT (PIT), IT services, and IT products.”

Note: Control systems are typically PIT

RMF PROCESS STEPS

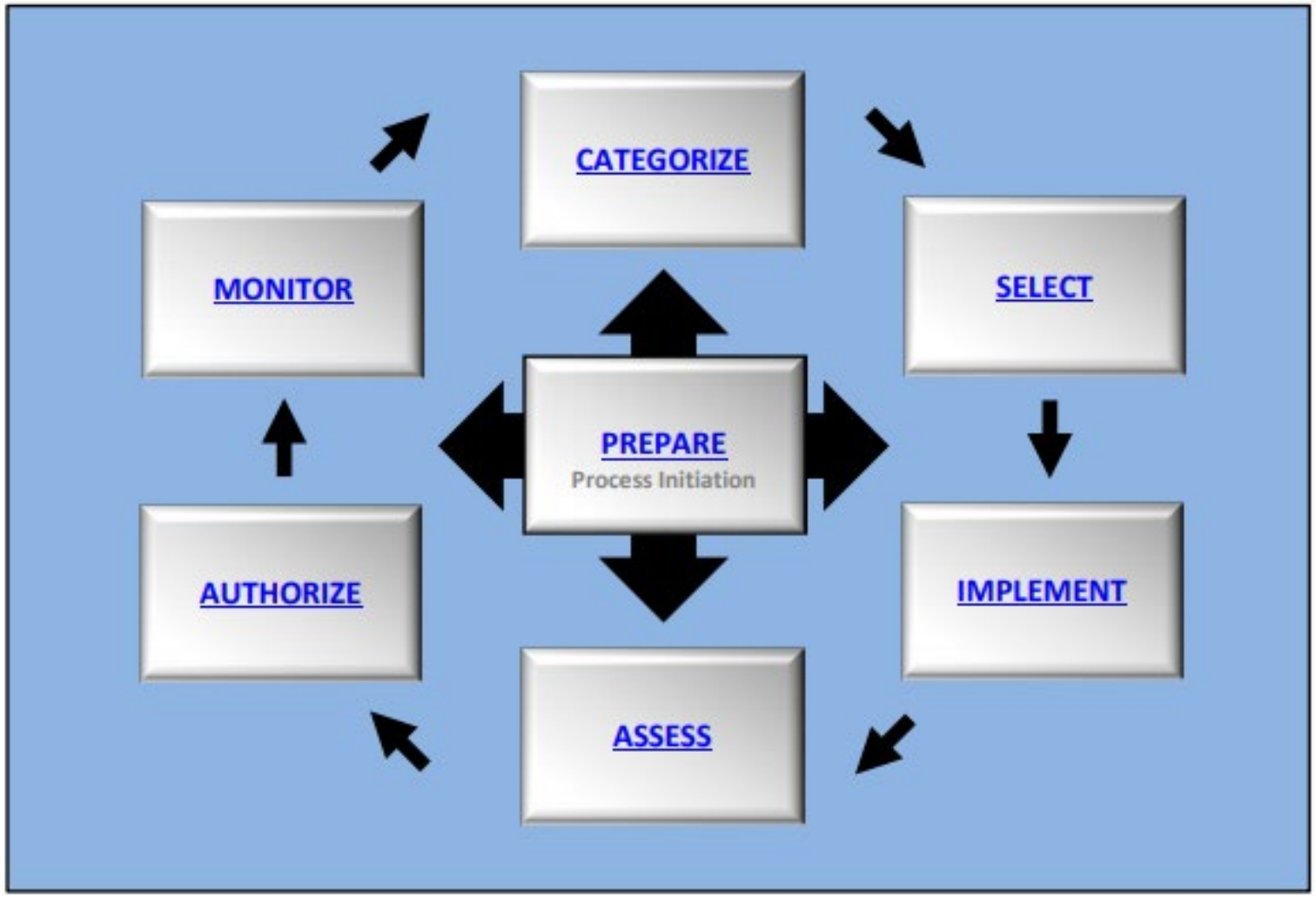


Image from NIST SP 800-37 R2

RMF KEY ROLES

- Authorizing Official (AO): Typically a General Officer or civilian equivalent who decides if a system is sufficiently secure to operate
- Security Control Assessor-Validator: The authorized entity who performs test and validation of the system IAW RMF security controls
- System Owner: Individual with overall responsibility for system implementation and security
- Information System Security Officer: The individual person responsible for system security

UFC 4-010-06 & UFGS 25 05 11: HOW THEY RELATE TO RMF

UNIFIED FACILITIES CRITERIA (UFC) 4-010-06

- Modified RMF process for the facility-related control system designer to follow
- Mostly applies to military construction projects
- CCIs are for systems categorized as Low or Moderate; High categorization is not considered by the UFC policy

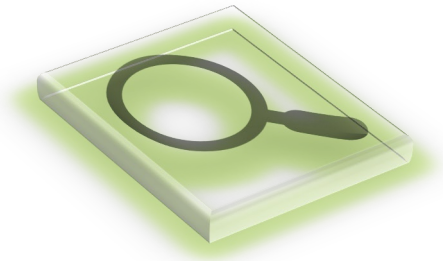
UNIFIED FACILITIES GUIDE SPECIFICATIONS (UFGS) 25 05 11

- Aids the GC in applying and meeting the cybersecurity requirements outlined in the UFC 4-010-06
- Simplified cybersecurity/RMF process, GC only provides pertinent submittals to the Govt customer for which the Govt customer is responsible for completing the RMF Assess & Authorize process
- Submittal examples include: Network Diagrams, Hardware/Software List, Password Summary Report, etc.

DECIPHERING GOVERNMENT REQUESTS FOR PROPOSALS (RFPs)

Excerpt taken from a Corps of Engineers RFP:

> 2.1 The Contractor shall provide a cyber-secure system with all applicable security artifacts and security engineering to meet the requirements of receiving an Authority to Operate (ATO) accreditation decision via the Department of Defense (DOD) Risk Management Framework (RMF). The design and construction of the system shall not favor functional requirements over security where possible. The expected duration for RMF Activities 1-5 stated below shall be approximately 12 months. The Contractor shall conduct and participate in RMF meetings as required by the PWS.



Does anything stick out to you?

- All applicable artifacts / security engineering
- ATO
- Shall not favor functionality over security
- 12 months

DECIPHERING RFPs (CONT'D)

Excerpt taken from a Corps of Engineers RFP:

> 8.5 Authority to Connect (ATC): Upon receipt of the final Security Authorization Determination, the Contractor shall assist the SO in obtaining ATC via network service provider (Network Enterprise Center (NEC), Directorate of Information Management (DOIM), Army Corps of Engineers IT (ACE-IT), or other Component / Service Branch (USN, USMC, AF, DLA, etc. Network Service Provider), if applicable. The Contractor shall follow the network service provider's criteria and process for ATC. 60 days should be allotted for completion.

ATC is needed when a system needs to connect to an external Government network.

If the system is a Standalone or Closed Restricted Network then an ATC is not needed.

Does an ATC requirement affect project schedule?

CONTRACTOR CYBER TASKS

Depending on the Cyber Requirements from the Gov't RFP, the contractor will likely need to perform the following tasks to achieve system ATO:

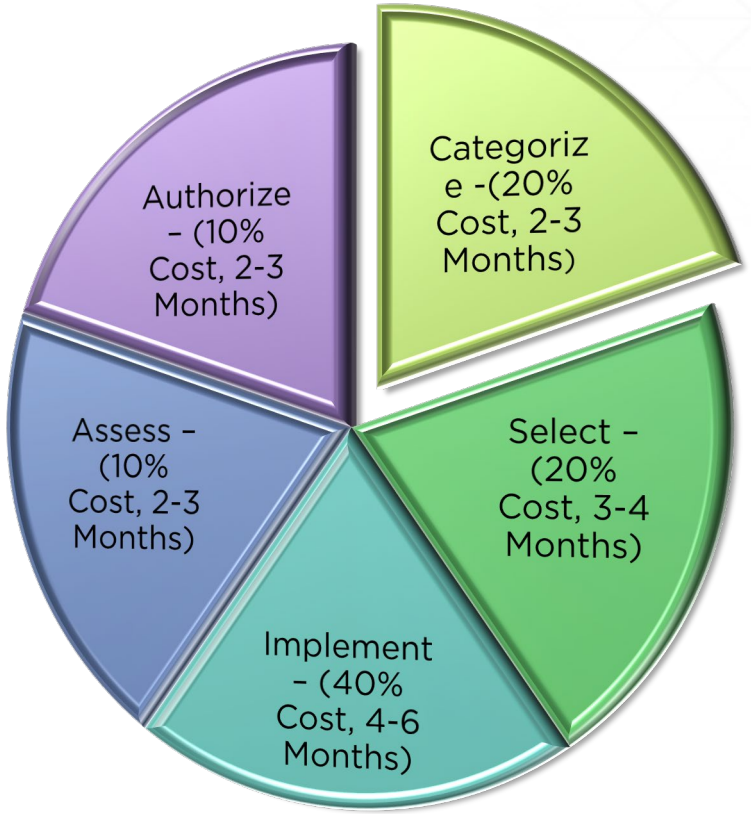
- ✓ *Design security architecture*
- ✓ *Perform Security Engineering of Hardware / Software*
- ✓ *Run SCAP and NESSUS scans*
- ✓ *Validate functionality of the system after hardening*

- ✓ *Develop the Security Plan and other RMF deliverables*
- ✓ *Create the Continuous Monitoring Plan*

- ✓ *Communicate with all Cybersecurity and System stakeholders*

- ✓ *Perform eMASS tasks*

SCHEDULE & COST IMPACTS
(NOT INCLUDING CONTINUOUS MONITORING)



ON AVERAGE, A TYPICAL RMF PROJECT TAKES 18 MONTHS DEPENDING ON GOVERNMENT ACTION/INACTION AND HOW THE SYSTEM IS ARCHITECTED…

CONCLUSION

- Existing cybersecurity requirements are being enforced to growing extent.
- Proactive steps have to be taken early, well before construction phase to ensure success.
- Without security authorization, your system will not be allowed to operate

TRIDIUM RESOURCES

Key Contact

- David Hornosky
- Email: david.hornosky@tridium.com
- Cell: (504) 912-3294

RMF Artifacts

- What are they?
- Who has access to them?
- DOD “SAFE” Application

Resources

- Collaboration with Experts in the Field
- Case Studies
- Documentation library (Niagara Community)
  https://www.niagara-community.com/Comm_Home

ALETA Technologies

TRIDIUM

QUESTIONS?

Todd Heflin
todd.heflin@aletatechnologies.com
256-895-8870

Herndon Elliott
herndon.elliott@aletatechnologies.com
256-895-8870

Jay Kurowsky
Jay.kurowsky@aletatechnologies.com
256-895-8870