Prototype to Production:

What do you need to know about ATO?

Brought to you by

NSTXL &

NATIONAL SECURITY TECHNOLOGY ACCELERATOR

DARK WOLF SOLUTIONS

DARK WOLF SOLUTIONS

Rick Tossavainen, Chief Executive Officer
rick.tossavainen@darkwolfsolutions.com

Tom Marlow, Deputy Director, Cybersecurity Practice
tom.marlow@darkwolfsolutions.com

Prototype to Production: what do you need to know about ATO?

Rick Tossavainen
CEO
Dark Wolf Solutions

rick.tossavainen@darkwolfsolutions.com

Tom Marlow
Deputy Director, Cybersecurity Practice
Dark Wolf Solutions

tom.marlow@darkwolfsolutions.com

What Is An ATO?

DARK WOLF SOLUTIONS

Information Security Authority to Operate

- An Authorization Official (AO) has assessed the risk of the information system and effectiveness of security controls to mitigate the risk, and has authorized the system to operate in production.
- The system gets to the decision point by completing the six steps of the Risk Management Framework (RMF).

ATO Types

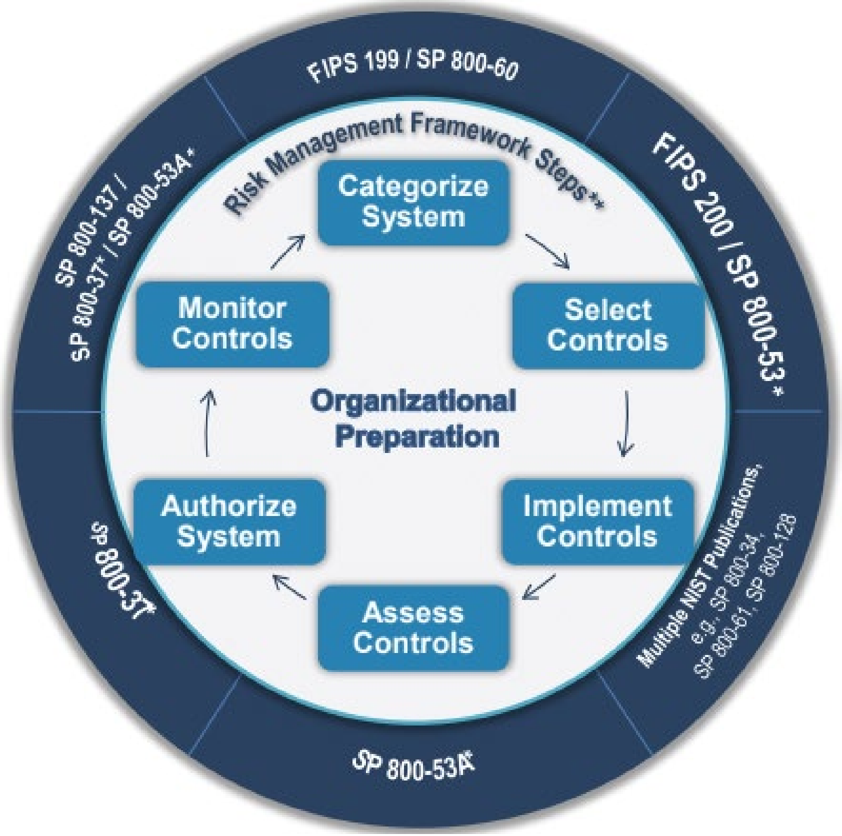
- **Traditional RMF**: a process that integrates security and risk management activities into the system development life cycle. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.
- **FT-ATO**: Fast Track ATO streamlines accreditation decisions by focusing on demonstrated security. Authorizing Officials must see evidence that a system adheres to standard cyber hygiene principles, has been validated through penetration testing, and has an Information System Continuous Monitoring (ISCM) strategy.
- **C-ATO**: For DevSecOps software factories with validated security policies and processes adhering to a Continuous ATO playbook, Continuous ATO facilitates automatic and immediate accreditation for all releases in compliance with Risk Management Framework requirements.

The Risk Management Framework

- A holistic and comprehensive risk management process.
- Integrated into the System Development Life Cycle (SDLC)
- Provides processes (tasks) for each of the six steps at the system level.

🟦 = Step

■ = Instructions to Complete the Step


FIPS 199 / SP 800-60
FIPS 200 / SP 800-53*
Multiple NIST Publications, e.g., SP 800-34, SP 800-61, SP 800-128
SP 800-53A*
SP 800-37*
SP 800-137 / SP 800-37* / SP 800-53A*
Risk Management Framework Steps**
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Organizational Preparation

NIST Standards: The Big 4

1. NIST Special Publication (SP) 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations*
   - Establishes the requirement for an ATO and the six steps of the RMF process.
2. Federal Information Processing Standard (FIPS) 199 - *Standards for Security Categorization of Federal Information and Information Systems*
   - Standard for categorizing information systems according to concerns for confidentiality, integrity, and availability. Used with SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.
3. FIPS 200 - *Minimum Security Requirements for Federal Information and Information Systems*
   - Provides a risk-based process for selecting the security controls necessary to satisfy the minimum requirements for information and an information system.
4. NIST SP 800-53 Rev 4 - *Security and Privacy Controls for for Federal Information Systems and Organizations*
   - Catalog of security and privacy controls.

RMF Step Details

DARK WOLF
SOLUTIONS

Categorize System

- Categorize system
- Initiate the System Security Plan
- Assign qualified personnel to RMF roles

Select Controls

- Identify common controls
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve the System Security Plan and ISCM strategy
- Apply overlays and tailor

Implement Controls

- Implement controls consistent with architecture and policies.
- Document security control implementation in the System Security Plan as a Control Matrix

Assess Controls

- Develop and approve Security Assessment Plan
- Assess controls
- Prepare control Test Report
- Conduct initial remediation actions

Authorize System

- Prepare the Plan of Action & Milestones (POA&M)
- Submit security authorization package
- AO coducts final risk determination
- AO makes authorization decision

Monitor Controls

- Analyze impact of major changes
- Assess selected controls annually
- Conduct remediation
- Update authorization package
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

Indicates significant artifact

Indicates action performed by the AO

OVERLAYS

- Overlays are additional control requirements driven by laws, regulations, and policies:
  - CNSSI 1253 - Controls to meet the requirements of National Security Systems
  - FedRAMP - Control requirements for cloud deployments
  - DoD Impact Levels - Control requirements established by DISA for DoD systems.
  - HIPAA - Federal privacy protections for individually identifiable health information.
  - PCI - Payment Card Industry security control requirements.
  - CMMC - Cybersecurity Maturity Model Certification establishes security control requirements for government contractors.

RMF Artifacts for ATO

1

System Security Plan
- System risk categorization
- Responsible organizations
- System Boundary
- Security Policies

2

Control Matrix
- Security Controls from NIST 800-53
- Implementation Details
- Crosswalk to other security requirements

3

Test Report
- Executive Summary
- Details of test procedures and results
- Detailed findings
- Residual risk summary

4

POA&M
- Task-oriented plan for closing vulnerabilities.
- Presents schedule
- Identifies accountable parties
- Living document

Submit questions:
www.slido.com
Code: X718

Fast Track ATO Background

Objectives

1. Provide an alternative pathway to ATO that better manages security risk by shifting the focus from exhaustive documentation of controls to the assessment of demonstrable cybersecurity in an operationally relevant environment.
2. Reduce the time required for an ATO when systems are transitioning to FedRAMP approved cloud environments.

Authority

- NIST SP 800-37 rev 2, *RMF for Information Systems and Organizations*
  - Incorporates *Supplemental Guidance on Ongoing Authorization*
  - Approval to Connect (ATC) remains at the discretion of the receiving AO, but reciprocity shall be used to the maximum extent possible.
  - If the operational environment is similar, the AO can use the existing adversarial assessment to inform their decision. Otherwise, the AO will require a new adversarial assessment.

FT-ATO Approach

18 March 2019 – Deputy CIO of Air Force signs "Fast-Track ATO" Memorandum

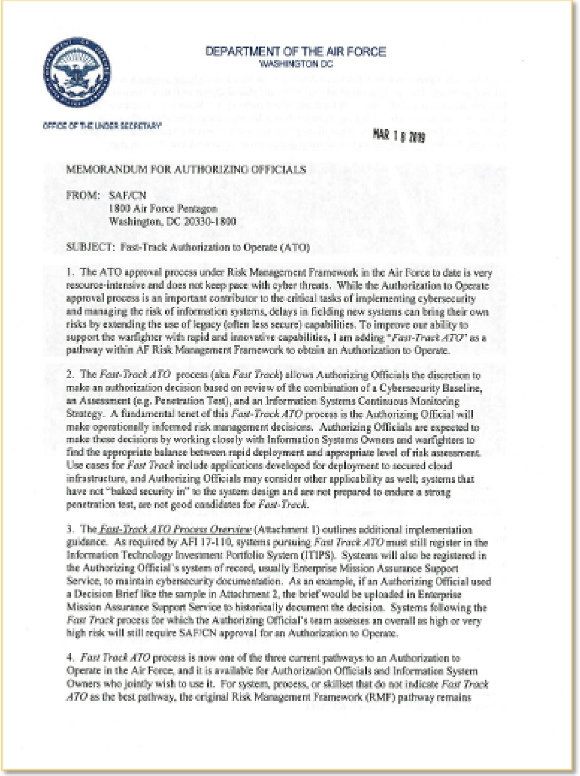
- "The ATO approval process under Risk Management Framework in the Air Force to date is very resource-intensive and does not keep pace with cyber threats."
- The AO is expected to make "operationally informed risk management decisions" based on three key elements.

Two attachments were included

- Fast Track Overview – Highlights some terms and high level direction
- Sample Decision Brief – Includes Risk Analysis Report

Fast Track does not remove/replace requirements to comply with Federal Mandates

- RMF & FISMA are still required
- System registration (e.g. ITIPS, eMASS) are still required
- Must perform adversarial assessment once environment is established



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

OFFICE OF THE UNDER SECRETARY

MAR 1 8 2019

MEMORANDUM FOR AUTHORIZING OFFICIALS

FROM: SAF/CN
1800 Air Force Pentagon
Washington, DC 20330-1800

SUBJECT: Fast-Track Authorization to Operate (ATO)

1. The ATO approval process under Risk Management Framework in the Air Force to date is very resource-intensive and does not keep pace with cyber threats. While the Authorization to Operate approval process is an important contributor to the critical tasks of implementing cybersecurity and managing the risk of information systems, delays in fielding new systems can bring their own risks by extending the use of legacy (often less secure) capabilities. To improve our ability to support the warfighter with rapid and innovative capabilities, I am adding "*Fast-Track ATO*" as a pathway within AF Risk Management Framework to obtain an Authorization to Operate.

2. The *Fast-Track ATO* process (aka *Fast Track*) allows Authorizing Officials the discretion to make an authorization decision based on review of the combination of a Cybersecurity Baseline, an Assessment (e.g. Penetration Test), and an Information Systems Continuous Monitoring Strategy. A fundamental tenet of this *Fast-Track ATO* process is the Authorizing Official will make operationally informed risk management decisions. Authorizing Officials are expected to make these decisions by working closely with Information Systems Owners and warfighters to find the appropriate balance between rapid deployment and appropriate level of risk assessment. Use cases for *Fast Track* include applications developed for deployment to secured cloud infrastructure, and Authorizing Officials may consider other applicability as well; systems that have not "baked security in" to the system design and are not prepared to endure a strong penetration test, are not good candidates for *Fast-Track*.

3. The *Fast-Track ATO Process Overview* (Attachment 1) outlines additional implementation guidance. As required by AFI 17-110, systems pursuing *Fast Track ATO* must still register in the Information Technology Investment Portfolio System (ITIPS). Systems will also be registered in the Authorizing Official's system of record, usually Enterprise Mission Assurance Support Service, to maintain cybersecurity documentation. As an example, if an Authorizing Official used a Decision Brief like the sample in Attachment 2, the brief would be uploaded in Enterprise Mission Assurance Support Service to historically document the decision. Systems following the *Fast Track* process for which the Authorizing Official's team assesses an overall as high or very high risk will still require SAF/CN approval for an Authorization to Operate.

4. *Fast Track ATO* process is now one of the three current pathways to an Authorization to Operate in the Air Force, and it is available for Authorization Officials and Information System Owners who jointly wish to use it. For system, process, or skillset that do not indicate *Fast Track ATO* as the best pathway, the original Risk Management Framework (RMF) pathway remains

Continuous ATO Background

Objectives

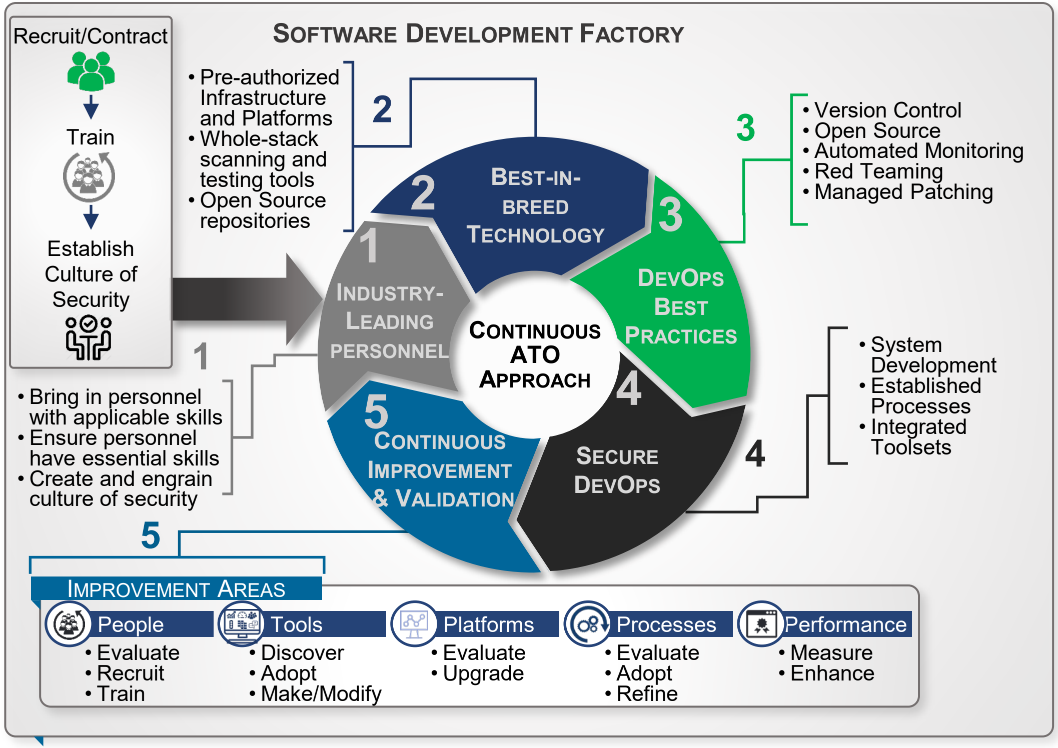
1. Enable a performance framework based on outcomes rather than compliance.
2. Reshape security processes to enable continuous integration and deployment.
    a. The current RMF process is designed for waterfall.
3. Create intrinsic software security
4. Accredits the platform and process and certifies the team that produces a product under a continuous monitoring process that maintains the residual risk within the risk tolerance of the AO

Authority

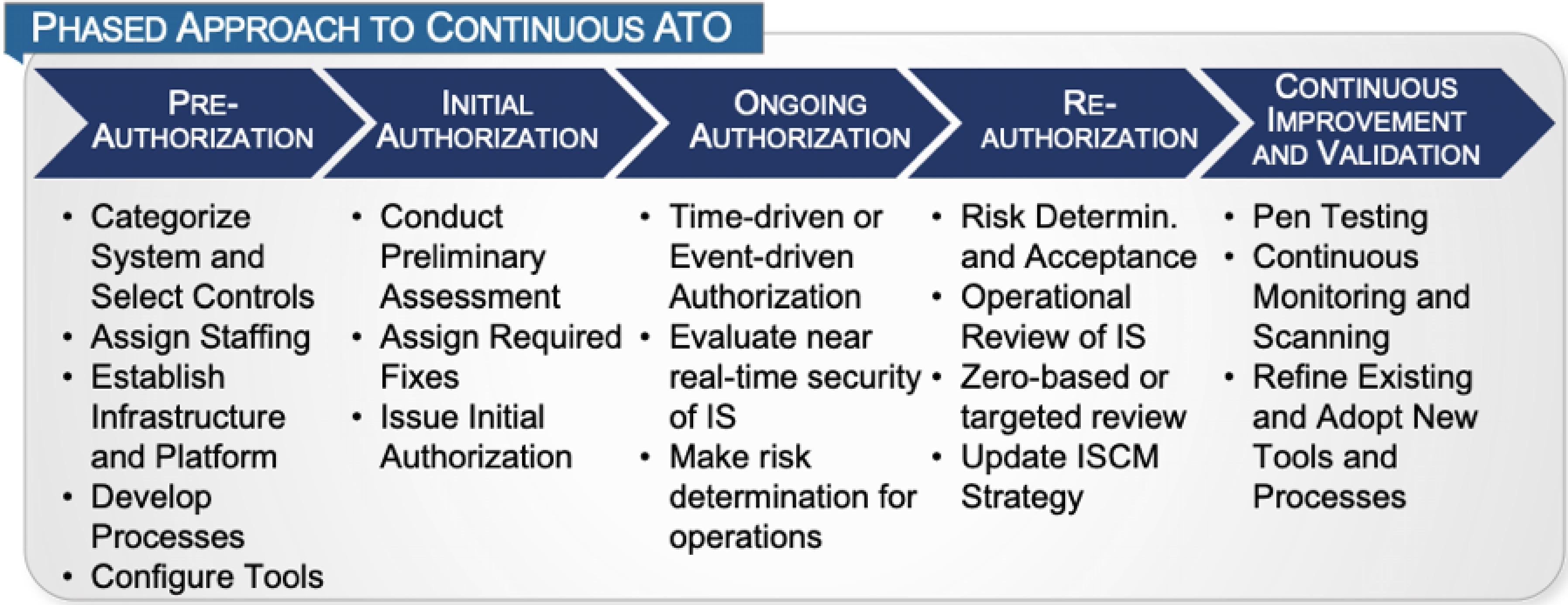
- NIST SP 800-37 rev 2, *RMF for Information Systems and Organizations*
    - Incorporates *Supplemental Guidance on Ongoing Authorization*

C-ATO Approach

- C-ATO begins with the establishment of a well designed and implemented software factory.
- There are five components that must be built into a software factory in order for C-ATO to work.
- By authorizing the factory, all applications developed within the factory will be granted ATO upon release to production.



C-ATO Steps



Phased Approach to Continuous ATO

Pre-Authorization

- Categorize System and Select Controls
- Assign Staffing
- Establish Infrastructure and Platform
- Develop Processes
- Configure Tools

Initial Authorization

- Conduct Preliminary Assessment
- Assign Required Fixes
- Issue Initial Authorization

Ongoing Authorization

- Time-driven or Event-driven Authorization
- Evaluate near real-time security of IS
- Make risk determination for operations

Re-Authorization

- Risk Determin. and Acceptance
- Operational Review of IS
- Zero-based or targeted review
- Update ISCM Strategy

Continuous Improvement and Validation

- Pen Testing
- Continuous Monitoring and Scanning
- Refine Existing and Adopt New Tools and Processes

Best Practices

Shift-left on Security

- Incorporate security in the earliest stages of your development
  - It’s much easier, faster, and cheaper to “bake in” security rather than “tack it on” at the end
- Create a “culture of security” - it is everyone’s business

Provide Transparency and Traceability to your AO

- Use tools such as SDElements or Xacta 360 and link them into your Git repo and requirements tracking system
  - Provides full mapping between requirement for RMF control, details of how that control was satisfied, and source code that satisfies that control

Professionalism throughout

- Spend extra time reviewing all documentation and ensuring alignment across all artifacts
- Answer questions from the AO as clearly and specifically as possible
- Be reasonable in your responses - your AO likely isn’t as technical as you and won’t have the most up-to-date information on your technical implementation - (ex. MySQL within RDS on C2S)

Working with the AO

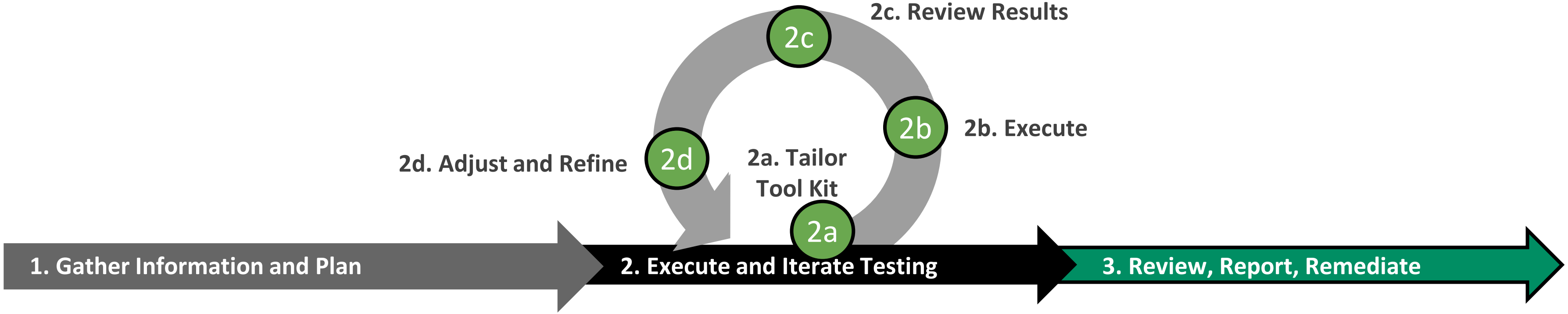
One size does not fit all

- Every AO is different and cares differently about degrees of risk
- Influencers: level of trust between the Development and Operations team, technical acumen, past experiences, willingness to lean forward and try new methods

Look for reciprocity opportunities

- Many AOs will accept reciprocity if the application, system, or component of the system was authorized by another government official, especially within the same agency or within DoD
- Using enterprise services for logging, authentication, and authorization can speed the process to ATO as many of the RMF controls are satisfied by these already accredited functions

Role of Penetration Testing



2c. Review Results
2c
2b
2b. Execute
2d. Adjust and Refine
2d
2a. Tailor Tool Kit
2a
1. Gather Information and Plan
2. Execute and Iterate Testing
3. Review, Report, Remediate

- Define scope and target systems
- Confirm rules of engagement
- Specify expected ATO inputs and exit criteria
- Assess network topology
- Cross-reference system architecture with common vulnerabilities and exposures
- Define plays to be employed

- Tailor custom tools to execute attacks and measure results
- Conduct a combination of automated testing, manual testing and manual verification
- Review results from each test iteration
- Adjust methods and scope to focus on critical findings

- Review tests and compare outcomes to expected results
- Assign risk factors
- Create reports and relevant ATO inputs
- Summarize possibilities for remediation approach
- Define scope of remediation efforts, if solicited
- Report suggested changes to policy, software, and network topology

THANK YOU!

Live Questions & Answers

DARK WOLF SOLUTIONS

Darkwolfsolutions.com

NSTXL

NATIONAL SECURITY TECHNOLOGY ACCELERATOR

NSTXL.org

DEFCON

2019: 2nd place Wireless Capture the Flag (CTF)

2017: 1st place IoT CTF

2016: 3rd place IoT CTF

BSIDES

2018: 1st place IoT Wireless CTF

2016: 1st place IoT CTF

2019 CYBERSECURITY IMPACT AWARDS

Leadership & Innovation Within the DMV cybersecurity industry.

LIVE Q&A

- Do we need to have a government sponsor in order to begin the process? If so, what does that look like?
  - Yes, although a longer answer is necessary, especially since it is highly AO dependent. For a little more detail: A government sponsor, primarily an AO along with a Government program that wants to use the product in production, will be necessary. However, you can begin the RMF steps while you secure the sponsorship of a Government official.
- When a fast track ATO is an option, who decides if it is an option?
  - We'll be sure to cover this in the Q&A portion of the session. The short answer is that it's particularly applicable in lift 'n' shift or lift transform and shift migrations. Specifically, when transitioning an accredited system from an accredited legacy architecture to an accredited cloud-based architecture. Usually, the AO will decide whether Fast Track is an acceptable option for arriving at an accreditation decision.

LIVE Q&A

- We currently are porting our software to Azure Government. Can we accelerate the ATO process by using the security/controls already baked into the secure cloud?
  - Yes, there should be nearly 100 controls that you can inherit through the Azure environment. We recommend reviewing Microsoft's "Azure Government Documentation", and specifically "Accelerate your path to ATO with Azure".

- Several USAF groups are using our sw in air-gapped mode; we've had difficulty finding the right AO, we keep getting passed around. Any advice to identify AO?
  - This is every system integrators nightmare. We'd like to talk offline and see if we can find someone to point you to. Please email us at rick.tossavainen@darkwolfsolutions.com and tom.marlow@darkwolfsolutions.com.

LIVE Q&A

- I've heard about the "party bus" approach to ATO. Does that only apply to cloud-based sw? Our solution is cloud + desktop component.
  - In these types of situations, we've seen separate ATOs completed for the desktop and cloud components. For the desktop, the organization usually wants to see a completed checklist that provides information about the application (i.e., software evaluation request, is the software COTS/GOTS, what mission does it support, and who are the POCs), a copy of the source code, and a compiled version that is run in a sandbox VM.
  - The cloud component would be a separate ATO that includes inherited controls from the cloud stack and platform being leveraged. We recommend working with AO to define the boundary of your software and requirements for RMF artifacts along with identifying the scans that need to be performed.
  - To discuss the requirements further, please email us at rick.tossavainen@darkwolfsolutions.com and tom.marlow@darkwolfsolutions.com

LIVE Q&A

- We are on a Phase 1 SBIR contract... and have a commercially viable product that is gaining ground in private sector --how should we plan for this in a Phase 2?
  - To plan for an ATO in Phase II, include milestones in your schedule to begin working with the AO of the production environment where you plan to install your software. We recommend meeting with the AO shortly after kick-off to bake security in throughout Phase II development process. Additional milestones for Phase II include the production of RMF artifacts, submission of package to ATO for review, execution of security control tests, and remediation of any vulnerabilities or POA&Ms to meet AO requirements for authorization.
  - Please email us at rick.tossavainen@darkwolfsolutions.com and tom.marlow@darkwolfsolutions.com to discuss further.
- We're a SBIR 2 company now - two pieces of guidance, 1) for sure build in the funds for working the ATO process 2) don't use vague language in your milestone
  - We agree; see our previous answer for milestone suggestions.

LIVE Q&A

- Any recommendations to ATO for very small systems such as one laptop?
  - There are many dependencies to consider: Will the laptop go into a secure environment, will it run classified data, and will it connect to a network. If you do not have an AO to talk with, please email us at rick.tossavainen@darkwolfsolutions.com and tom.marlow@darkwolfsolutions.com. We believe that the laptop should be STIG'd at a minimum.
- Any advice for getting ATOs with virtual and augmented reality headsets?
  - There are many dependencies to consider, for example, do the headsets have built-in microphones for noise cancelling? Are there built in cameras? Will they connect to and run in a secure environment? Who manufactures the headset, and what is the supply chain risk in the components that are used? If you would like to discuss the AO's potential questions further, please email us at rick.tossavainen@darkwolfsolutions.com and tom.marlow@darkwolfsolutions.com.

LIVE Q&A

- What is a good source for downloading templates (security plan etc)?
  - There are a couple of resources you can check for templates. These may be complimented by agency or program specific requirements:
  - NIST Resources: https://www.nist.gov/cyberframework/federal-resources
  - FedRAMP SSP Templates that can be adapted to general RMF: https://www.fedramp.gov/developing-a-system-security-plan/
  - NIST SP 800-18 Appendix A provides the very basics: https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final

- Please email us at rick.tossavainen@darkwolfsolutions.com and tom.marlow@darkwolfsolutions.com to talk further about potential templates.

LIVE Q&A

- I assume Dark Wolf provides ATO-as-a-Service (couldn't resist). Can you provide a ROM for Dark Wolf to assist a vendor to get an ATO?
  - Please email us at rick.tossavainen@darkwolfsolutions.com and tom.marlow@darkwolfsolutions.com to talk further about ROMs to assist with the ATO process.
- Do you have scaled down service offerings for small non-traditional tech start ups that are working with PRIMEs as a sub contractor, etc.?
  - We support organizations of different sizes and contract relationships. We can help you determine the appropriate level of support that you need. Please email us at rick.tossavainen@darkwolfsolutions.com and tom.marlow@darkwolfsolutions.com to talk further.

LIVE Q&A

- How difficult is it to stand up and have the capability of helping companies get an ATO?
  - This is a capability we've been building for over 5 years, and we evolve it as regulations, client expectations, and technologies change. It requires constant care and feeding. We participate in numerous hacking competitions throughout the year throughout the U.S to keep our skills sharp. For more information, please email us at rick.tossavainen@darkwolfsolutions.com and tom.marlow@darkwolfsolutions.com

THANK YOU!