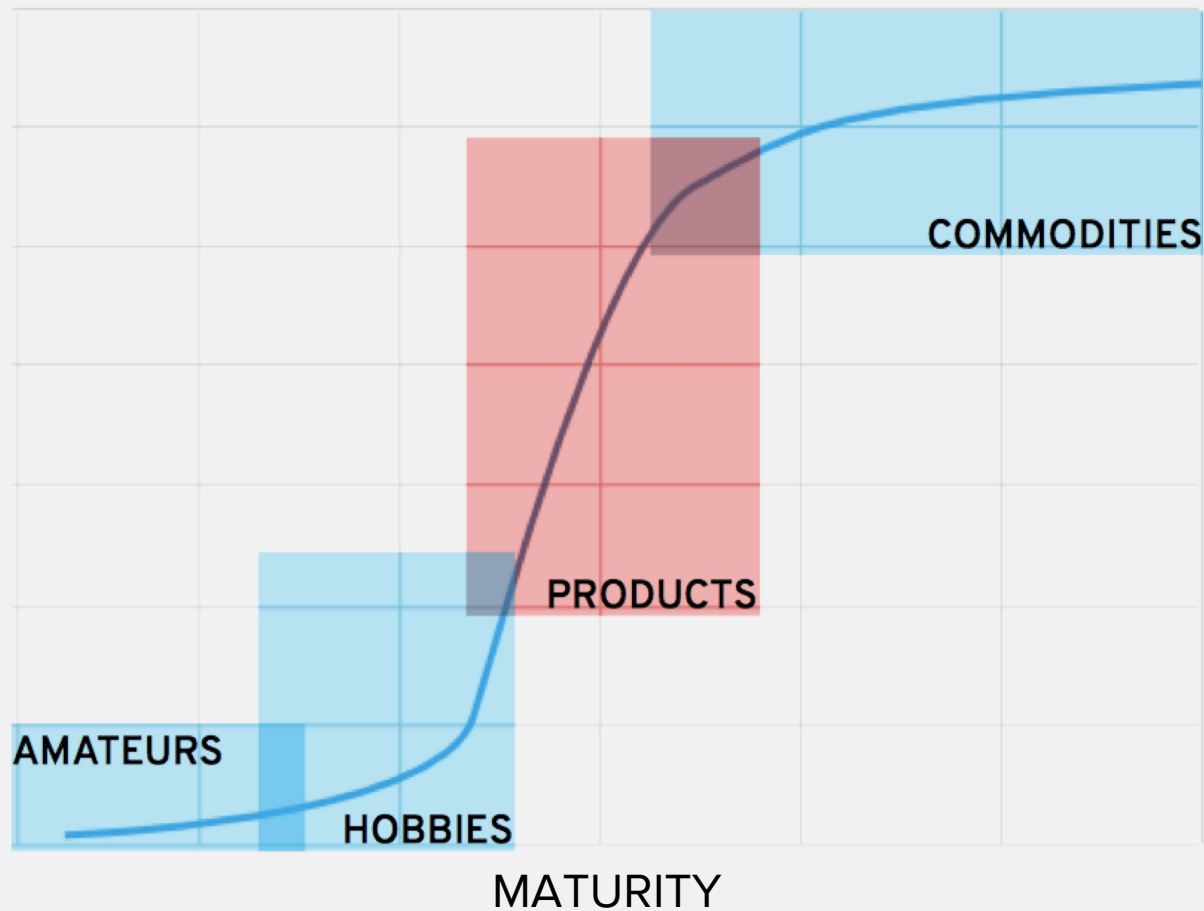




# Aligning & Sharing Cybersecurity Practices Between Federal and State

Shawn Wells  
Chief Security Strategist  
U.S. Public Sector  
shawn@redhat.com || 443-534-0130

UBIQUITY



# FISMA from an earlier era

- Originally authored in 2002
- Pre GovCloud, C2S, MilCloud
- Pre DevOps, Infrastructure as Code
- Multi-year dev/ship cycles common
- Waterfall dominant
- IT was more manual a decade ago



# Lessons from industry: ORock

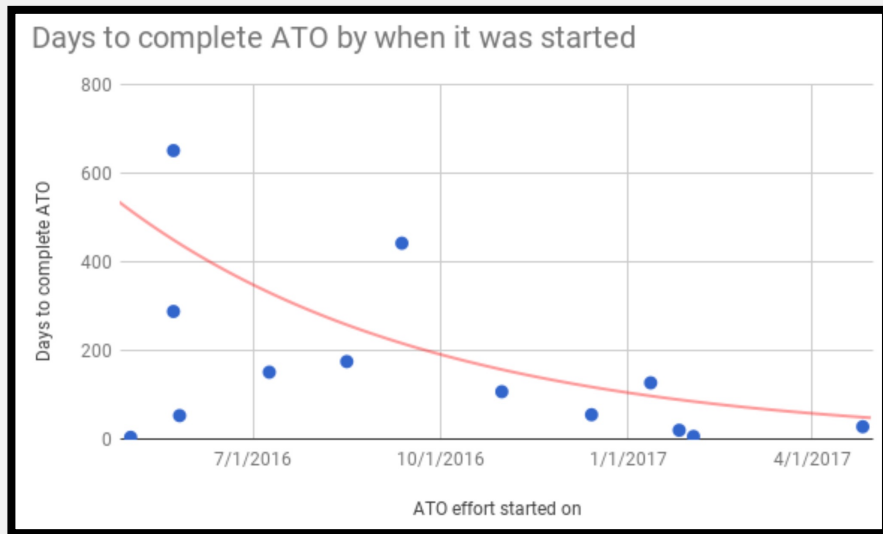
FedRAMP ATO in four months.



# Lessons from Government: 18F

**“With the new process, we have cleared the backlog and reduced the turnaround time to under a month. We think that deserves a celebration and makes for a good opportunity to share the lessons we’ve learned.”**

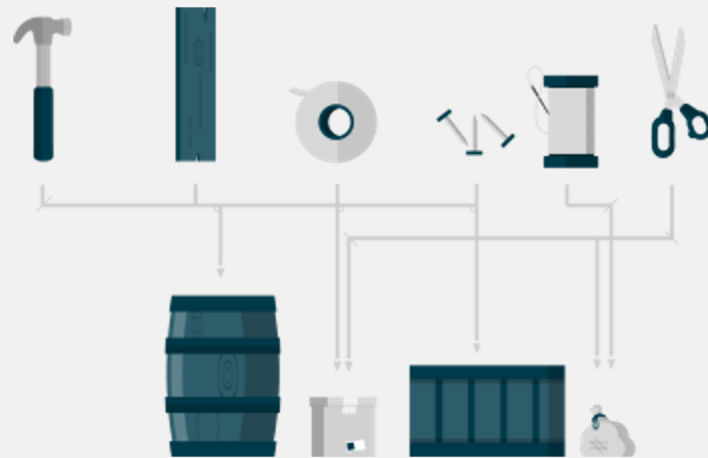
- Aidan Feldman, 18F



# A Challenge

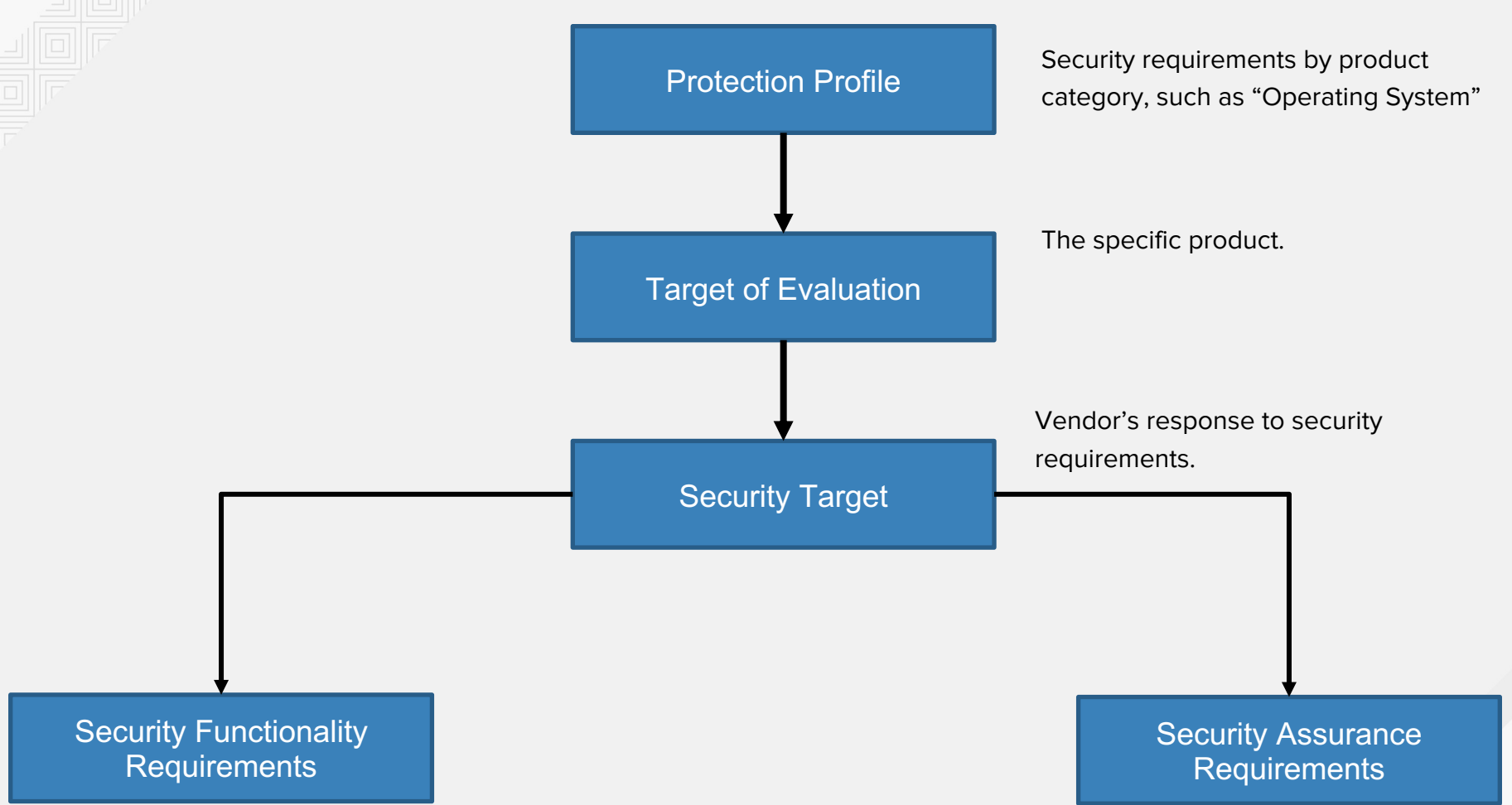
The FAA was encumbered by verifying security of system components upon receipt from system integrators.

How could security be moved to an acquisition requirement?





Common Criteria (CC) is an international set of guidelines and specifications developed for evaluating information security products, specifically to ensure they meet an agreed-upon security standard for government deployments





Tech Type ▲	Profile Name ◆	CC Ver. ◆	Short Name ◆
Application Software	Protection Profile for Application Software Version 1.2	3.1	PP_APP_v1.2
BIOS Update	Protection Profile for BIOS Update for PC Client Devices Version 1.0	3.1	PP_BIOS_v1.0
Certificate Authority	Protection Profile for Certification Authorities Version 2.1	3.1	PP_CA_V2.1
Email Client	Extended Package for Email Clients v2.0	3.1	PP_APP_EMAILCLIENT_EP_v2.0
Encrypted Storage	collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition Version 2.0	3.1	CPP_FDE_AA_V2.0
Encrypted Storage	collaborative Protection Profile for Full Drive Encryption - Encryption Engine Version 2.0	3.1	CPP_FDE_EE_V2.0
Encrypted Storage	Extended Package for Software File Encryption Version 1.0	3.1	PP_APP_SWFE_EP_v1.0

<https://www.niap-ccevs.org/Profile/PP.cfm>

## 2. Configuration Requirements

The table below describes configuration requirements for operating systems.

Each configuration requirement is associated with a security functionality requirement (SFR) from the associated Protection Profile or Module. Each configuration requirement is also associated with a NIST 800-53 security control and CNSSI 1253 configuration value where applicable. See Wireless EP/Module for wireless-specific configuration requirements.

Configuration Action	NIST Control	CNSSI 1253 Value or DoD-specific Value	NIAP PP Reference
Configure Minimum Password Length to 12 Characters	IA-5 (1)(a)	12 characters	FMT_MOF_EXT.1
Require at Least 1 Special Character in Password	IA-5 (1)(a)	at least one	FMT_MOF_EXT.1
Require at Least 1 Numeric Character in Password	IA-5 (1)(a)	at least one	FMT_MOF_EXT.1
Require at Least 1 Uppercase Character in Password	IA-5 (1)(a)	at least one	FMT_MOF_EXT.1
Require at Least 1 Lowercase Character in Password	IA-5 (1)(a)	at least one	FMT_MOF_EXT.1
Enable Screen Lock	AC-11a.		FMT_MOF_EXT.1
Set Screen Lock Timeout Period to 30 Minutes or Less	AC-11a.	30 minutes	FMT_MOF_EXT.1
Disable Unauthenticated Login (such as Guest Accounts)			FIA_AFL.1
Set Maximum Number of Authentication Failures to 3 Within 15 Minutes	AC-7a.	3 15 minutes	FMT_MOF_EXT.1
Enable Host-Based Firewall	SC-7 (12)		FMT_MOF_EXT.1
Configure Name/Address of Remote Management Server From Which to Receive Config Settings	CM-3(3)		FMT_MOF_EXT.1



# A Challenge

Army Cyber required dozens of applications for defensive operations.

Those applications required complicated collaboration during installation and integration every time they were deployed.



**OMB's FISMA problem.**

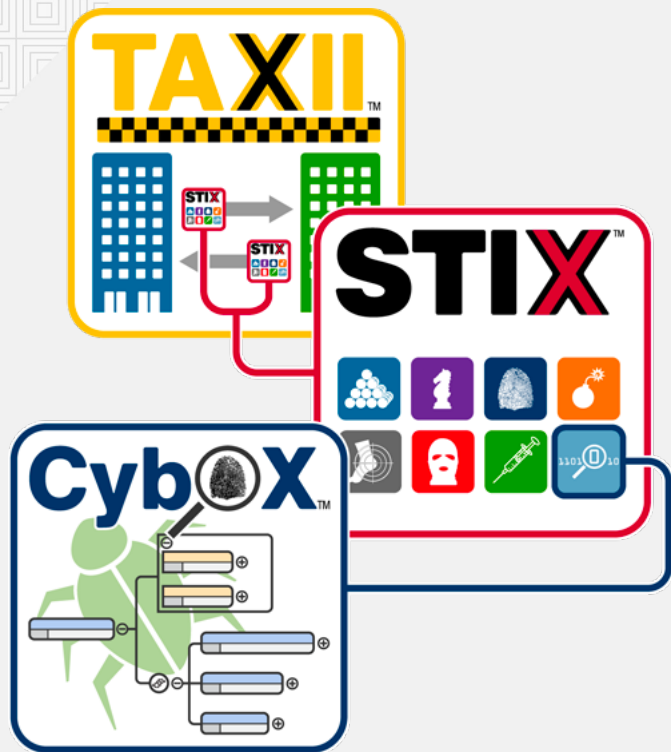
## National Checklist Program Repository

The National Checklist Program (NCP), defined by the [NIST SP 800-70](#), is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications.



How can we share cyber insights? How can we create a government-wide awareness of cyber events?











TAXII:  
Trusted Automated eXchange of  
Indicator Information

STIX:  
Structured Threat Information  
eXpression

CybOX:  
Cyber Observable eXpression

# Emerging Technology: OpenControl

## Requirements Traceability Matrix

Control	Name	Status
<a href="#">AU-1</a>	Audit And Accountability Policy And Procedures	 not applicable
<a href="#">AU-2</a>	Audit Events	 not applicable
<a href="#">AU-3</a>	Content Of Audit Records	 complete
<a href="#">AU-4</a>	Audit Storage Capacity	 not applicable
<a href="#">AU-4 (1)</a>	Transfer To Alternate Storage	 none
<a href="#">AU-5</a>	Response To Audit Processing Failures	 planned



# Thank you!

E-Mail: shawn@redhat.com

LinkedIn: <https://www.linkedin.com/in/shawndwells/>

Cell: 443-534-0130 (US EST)

