Acronis SCS

DoDIN APL:
A Labor of Love

John Downey
VP of Sales
JD@AcronisSCS.com

Neil Proctor
VP of Engineering and R&D
NP@AcronisSCS.com

Agenda

Who We Are

DoD Cyber Challenges

Lists, Lists, and more Lists

Our Experience: FIPS 140-2, Common Criteria, and DoDIN APL

Bottom Line

Q & A

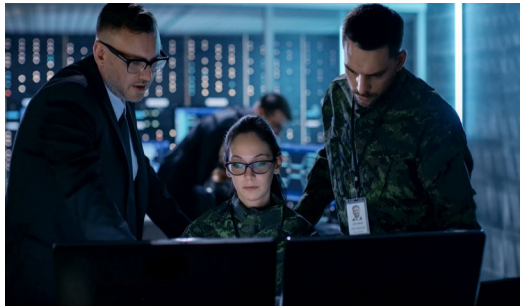
Acronis SCS

A trusted, US cyber protection company dedicated to the public sector

Scottsdale, Arizona HQ

All employees are US citizens

Public Sector Commitment



Uniquely positioned to work hand in hand with local, state & federal organizations

Proven Track Record

15 years of product service to the public sector including all branches of the military

- 15-year product history
- Dedicated public sector products
- Innovating on supply chain transparency
- Serving nearly 40,000 US public sector organizations

Government Cybersecurity Landscape

"DoD cybersecurity is at a critical juncture. Its networks are growing in size and complexity, requiring **massive amounts of rapid data transfer** to maintain situational awareness on the digital and physical battlefield. This expansion is stretching existing cybersecurity apparatuses to their breaking point, as an **ever-growing number of users and endpoints increases the attack surface** of the network."
- 2019 Defense Innovation Board Whitepaper

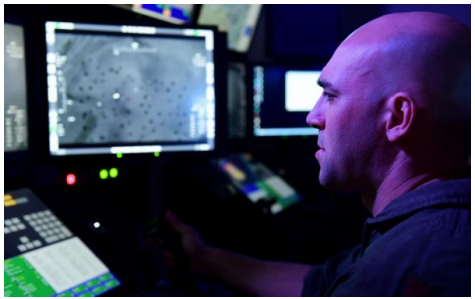
- What we hear about in the media: data breaches, data breaches, data breaches
  - Compromise or loss of sensitive information, including PII
- This is important, but our focus is different...
- We're centered on **operational assurance**:
  - Minimizing or **eliminating downtime** to ensure access to **mission critical** data and systems
  - Keeping DoD and other government agency systems up and running in the face of attack or failure

Where we sit on the DoD's Unique Edge…

Often operating in "no internet" environments with classified / sensitive information

Mobile Endpoints

Testing & Training



In Theater

Cyber Challenges… In DoD's Words

Diverse cyber threat landscape – only growing in scale and scope

DoD's "networks must be mobile enough to support missions around the world, and flexible enough to facilitate collaboration with any partners a mission requires, expected or unexpected."

- 2019 DoD Digital Modernization Strategy

"Space and cyber have now emerged as new warfighting domains. And while technological progress in these areas has generated great opportunity, it has also created vulnerabilities that our adversaries seek to exploit."

- Mark Esper, Secretary of Defense

"When I think about cloud and AI, and all of the advanced capabilities we want to bring to the warfighter, I think about making sure the warfighter has the right comms and the right information at the right time."

- Dana Deasy, DoD CIO

"We have a great deal of standards for cybersecurity. What we are lacking is a unified standard... If we were doing all the necessary security controls, we wouldn't be getting exfiltrated to the level that we are."

- Katie Arrington, DoD Special Assistant for Cyber Acquisition

Lists, Lists… & More Lists

A false choice between product operability and security?

- DITPR - Department of Defense Information Technology Portfolio Repository
  - Used by all DoD components to maintain a comprehensive, consolidated inventory of unclassified, mission-critical, and mission-essential systems
- DADMS - Department of the Navy Application and Database Management System
  - DADMS, the Navy's platform for DITPR, is their single, authoritative source and web-based registry for Navy and Marine Corps systems, applications, databases, networks, and server information
- APMS - Army Portfolio Management Solution, AGM - Army Golden Master, and Army CON - Certificate of Networthiness
  - APMS, the Army's platform for DITPR, is the authoritative data source for the Army's inventory of active IT investments, associated systems, and applications, as well as information system and application hosting environments
  - The Army Golden Master (AGM) list provides operating systems and utility programs on Army desktop machines
  - Army Certificate of Networthiness Program (CON) is concerned with the identification, measurement, control, and minimization of security risks and impacts in IT systems to a level commensurate with the value of the assets protected
- Air Force Guidance
  - The Air Force provides a list of lists to consult depending on the type of technology being purchased
- ATO - Authority to Operate
  - Formal declaration that authorizes operation of a Business Product and explicitly accepts the risk to agency operations. Documents the security measures taken and the security process in place for US federal government agencies by focusing on a specific system

Why Choose Certified Products?

These stacked certifications are the gold standard of security & interoperability

FIPS

- Key Testing / Requirements:
  - Approved algorithms & cryptographic module specifications to protect sensitive information
  - Random number & key generation for maximum entropy

Common Criteria

- Application Software Key Testing / Requirements:
  - Cryptographic support
  - User data protection
  - Security management
  - Protection of the TSF
  - Privacy
  - Trusted path / channel
- NIAP standards managed by NSA & accepted by 31 countries

DoDIN APL

- Key Testing / Requirements:
  - Cryptography
  - Information Assurance
  - CAC/PKI
  - IPv6
  - UCR Requirements
  - CS Testing
  - SAR Testing
  - IO Testing

FIPS 140-2

Our Journey and Challenges

Importance of FIPS: Explicitly provides the details around how systems use encryption and which encryption algorithms are verified to be secure

Our FIPS Challenges:

- Default entry point and the way the power on self tests work
- RSA key generation probable primes
- Integrate new FIPS compatible library into our application

Common Criteria

Our Journey and Challenges

Importance of Common Criteria: Focuses on the application in its entirety and its operational environment. It outlines the details of how you need to secure your communication.

Our Common Criteria Challenges:

- Protection profiles you submit under do not always match what your product does
    - Protection Profile – Application Software
- How the PKI and certificate authority checks were handled
- How an application must store secrets – root level credential
- How we compile code – buffer overflow and dynamic memory allocation

DoDIN APL

Our Journey and Challenges

Importance of DoDIN APL: Adherence with operational parameters regarding users and making sure all the logging is occurring and sent to a single location

Our DoDIN APL Challenges:

- STIGs regarding logging, user access, banners, cookie properties, etc.
- A LOT of STIGs and they get VERY detailed

The DoDIN APL has been referred to by many names, including the UC APL (Unified Capabilities Approved Products List), JITC and STIG Testing, and more

As part of your certification, you must also complete: FIPS 140-2 and Common Criteria

Bottomline:

The DoDIN APL is the gold standard for security AND operability…

Now how can we ensure it's the go-to choice and not the stick in the tire?

- DoD and private sector time to market
- Guidance is minimal compared to the level of specification
- Working implementations aren’t shared as examples

Acronis SCS

Thank You!

For more information, visit
www.AcronisSCS.com