How Cybersecurity is Changing Test Engineering

Steve Summers
Security Lead, ADG

Kyle Tetmeyer
Security Program Manager

Joe Jarzombek
SCRM & Software Assurance SME

Presenters

Steve Summers

- NI ADG Security Lead

Kyle Tetmeyer

- NI Chief Program Manager, Product Security

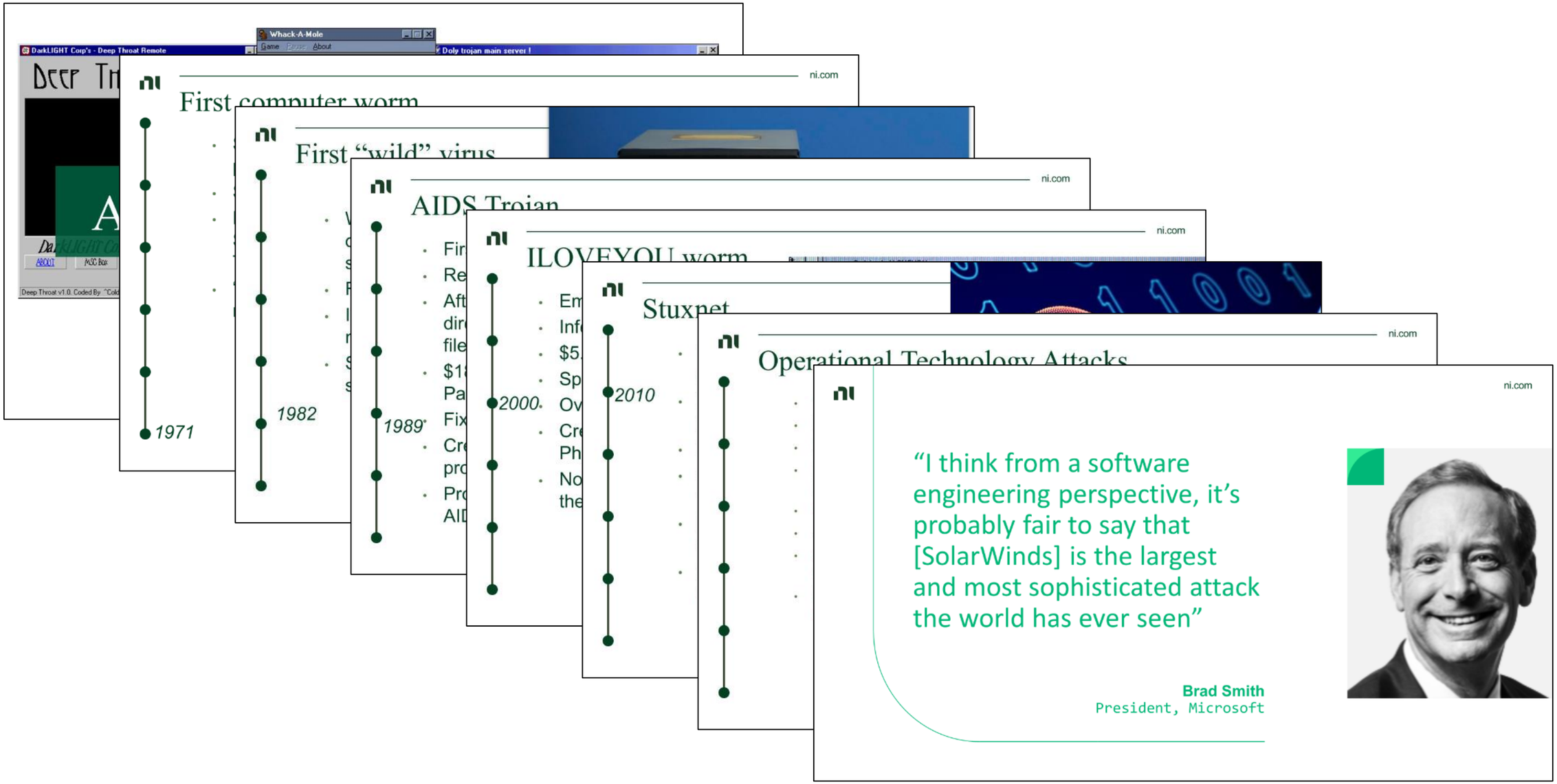
Steven Harrison

- NI Sr Director, R&D SW
- Security Officer

Joe Jarzombek

- SCRM & Software Assurance SME
- Ret. AF, DHS, Pentagon SW Security

Cybersecurity Threats



Cybersecurity Threats – 2023 update

2023:

- 60% increase in interactive intrusion campaigns *(executing actions on host)*
- Most targeted sector: Technology (23% of attacks)
- Most targeted country: US (61% of attacks)
- Attacks not using Malware: 75% (social engineering, phishing, access brokers)
- 76% increase in victims named on eCrime leak sites
- Average breakout time: 62 minutes (down from 87 minutes) *fastest: 2 min 7 sec*
- Total Ransomware attacks: Up 84% over 2022 to 4,667 cases
- More than $1B ransom paid in 2023

Cybersecurity Threats – 2024 update

Blackjack infrastructure attack

https://claroty.com/team82/research/unpacking-the-blackjack-groups-fuxnet-malware

Ukrainian attack on Russian infrastructure (water/sewer)

Claimed by the attackers:

- Disabled up to 1,700 sensor-gateways
- Fuzzed or disabled up to 87,000 sensors
- Gained access to Russia's emergency service number
- Disabled network appliances
- Deleted servers, workstations, databases (30 TB)
- Disabled access to utility office building
- Dumped passwords from multiple internal services

Does security matter to test?

2008: Mocmex virus

- Designed to work around firewalls and security software
- Downloads files from remote locations
- Hides and randomly renames files
- Spreads through portable storage devices

- Hides on firmware in digital photoframes, spreads on home networks

- How did this get into the photoframes?
- *Installed from infected testers*

Evolution of a Cybersecurity Attack

Initial Access	Persistence	Privilege Escalation	Credential Access	Lateral Movement	Exfiltration	Impact
Obtain credentials	Achieve identity persistence	Modify policies /add identities	Harvest additional credentials	Move among targets	Download data	Use data to monetize

A modern cybersecurity strategy has to prepare for every stage of an attack

EMERSON

Zero Trust Principles

Microsoft Security

Verify explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Use least-privilege access

Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Assume breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

EMERSON

Zero Trust Example – Airport Security

Ticket Counter

Authenticate (ID)
Authorize (Ticket)
X-ray Bags

Security Checkpoint

Authenticate (ID)
Authorize (Ticket)
X-ray Person & Bags

Baggage Handling

Controlled Access

Gate

Authorize (Ticket)

Cockpit

Controlled Access

Pilot

Access (ID)

Government Action - Europe

European CRA
https://www.european-cyber-resilience-act.com/

First proposed September 2022
Passed in March 2024
Waiting on Formal Adoption – May 2024

Key Elements:

- Required for import to the EU
- Applies to any hardware or software expected to connect to another device or network
- Will require new CE mark asserting compliance with security standards
- Companies will have 21 & 36 months to fully comply

EU CRA Security Standards

European CRA
https://www.european-cyber-resilience-act.com/

- Develop with secure development principles
- Provide security related information with logging
- Reduce impact of an incident
- Release product with no known exploitable vulnerabilities
- Release with secure-by-default configuration
- 5-year security support cycle
- Conduct cyber risk assessment
- Cooperate with market surveillance authorities
- Manage supply chain for security
- Maintain SBOM for each device
- Fix vulnerabilities
- Public disclosure of vulnerabilities, fixes

Government Action – US Government

Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing

Expected to be released in May 2024:

- Contractors must generate SBOM for any software “used in performance of a contract”
- Cooperate with CISA on any cyber investigation
- Report cyber incidents to CISA within 8 hours
- Comply with all-IPv6 network requirements

NATIONAL ARCHIVES

FEDERAL REGISTER

The Daily Journal of the United States Government

Proposed Rule

Government Action – US DoD

Cybersecurity Maturity Model Certification - CMMC

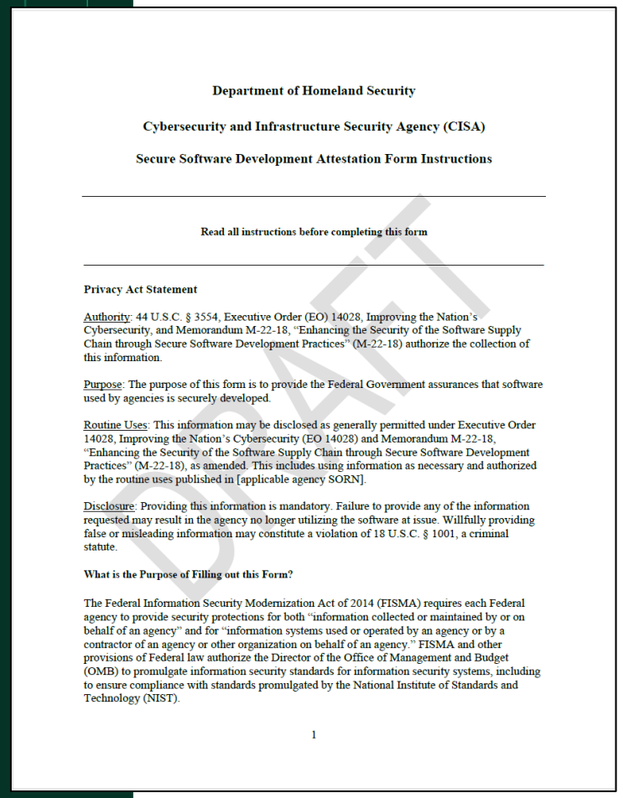
Release expected October 2024

Systems processing Government Data must comply with NIST 800-171 controls

17 control families, 110 controls:

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Configuration Management
5. Contingency Planning
6. Identification and Authentication
7. Incident Response
8. Maintenance
9. Media Protection
10. Personnel Security
11. Physical Protection and Environmental Protection
12. Planning
13. Program Management
14. Risk Assessment
15. Security Assessment and Authorization
16. System and Communications Protection
17. System and Information Integrity

Government Action – DHS CISA



Department of Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

Secure Software Development Attestation Form Instructions

Read all instructions before completing this form

Privacy Act Statement

Authority: 44 U.S.C. § 3554, Executive Order (EO) 14028, Improving the Nation's Cybersecurity, and Memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" (M-22-18) authorize the collection of this information.

Purpose: The purpose of this form is to provide the Federal Government assurances that software used by agencies is securely developed.

Routine Uses: This information may be disclosed as generally permitted under Executive Order 14028, Improving the Nation's Cybersecurity (EO 14028) and Memorandum M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" (M-22-18), as amended. This includes using information as necessary and authorized by the routine uses published in [applicable agency SORN].

Disclosure: Providing this information is mandatory. Failure to provide any of the information requested may result in the agency no longer utilizing the software at issue. Willfully providing false or misleading information may constitute a violation of 18 U.S.C. § 1001, a criminal statute.

What is the Purpose of Filling out this Form?

The Federal Information Security Modernization Act of 2014 (FISMA) requires each Federal agency to provide security protections for both "information collected or maintained by or on behalf of an agency" and for "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." FISMA and other provisions of Federal law authorize the Director of the Office of Management and Budget (OMB) to promulgate information security standards for information security systems, including to ensure compliance with standards promulgated by the National Institute of Standards and Technology (NIST).

1

DRAFT

I attest that [software producer] presently makes consistent use of the following practices, drawn from the secure software development framework (SSDF) in developing the software

GSA 7700 Attestation Form

https://www.gsa.gov/reference/forms/secure-software-development-attestation

- To ensure a safe and secure digital ecosystem for all Americans, CISA released the Secure Software Development Attestation Form on March 11, 2024, taking a major step in the implementation of its requirement that producers of software used by the Federal Government attest to the adoption of secure development practices.
  - CISA developed this form in close consultation with the Office of Management and Budget (OMB) and based upon practices established in the National Institute of Standards and Technology's Secure Software Development Framework (SSDF).
  - The release of the secure software development attestation form reinforces secure by design principles advanced by CISA, Federal government partners, and international allies.
  - As a step on this journey, Executive Order 14028 and the OMB M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, and OMB M-23-16, Update to Memorandum M-22-18,* required development of an attestation form in which software producers serving the federal government will be required to confirm implementation of specific security practices.

EMERSON

Government Action – DHS CISA

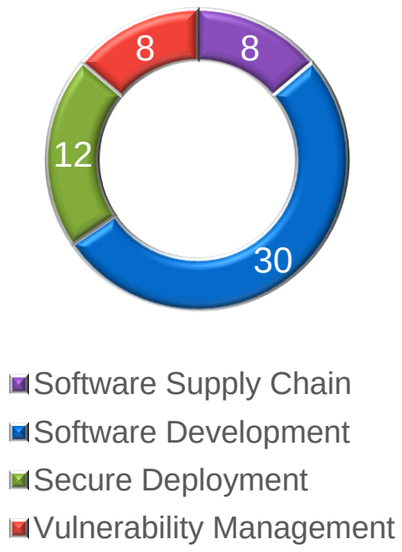
Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle

Developed in collaboration with government/industry ICT SCRM Task Force, focuses on ***'secure by demand' -- customer expectations for secure software and products are articulated in acquisition and procurement activities and contracts.***

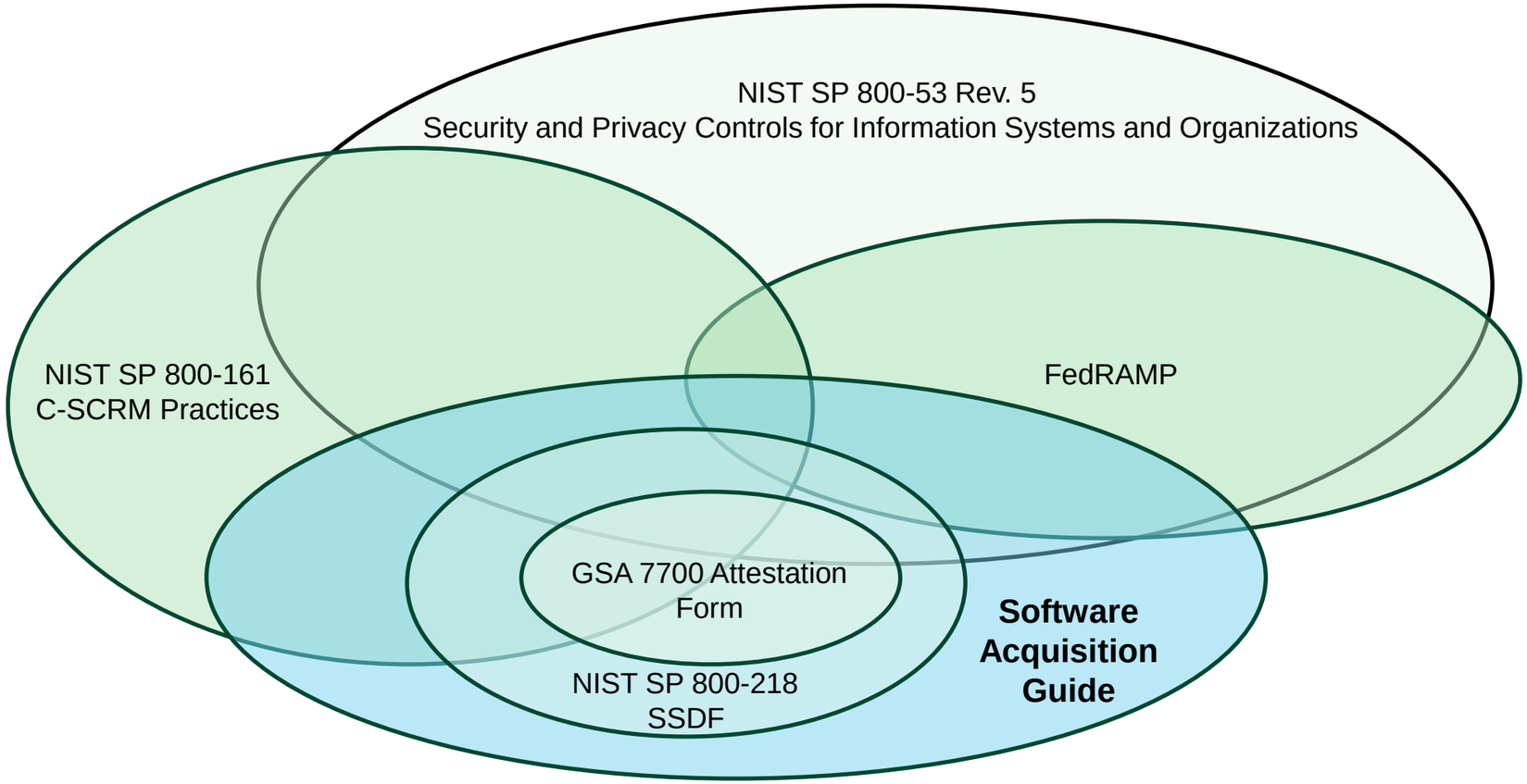
- 25 control questions could be skipped if the supplier provides a CISA Secure Software Development Attestation Form without the need for a POA&M.
- Affirmatively answering all 19 Supplier Governance and Attestation questions enables all remaining CONTROL questions in each control category to be skipped in subsequent sections of the guide.

Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle

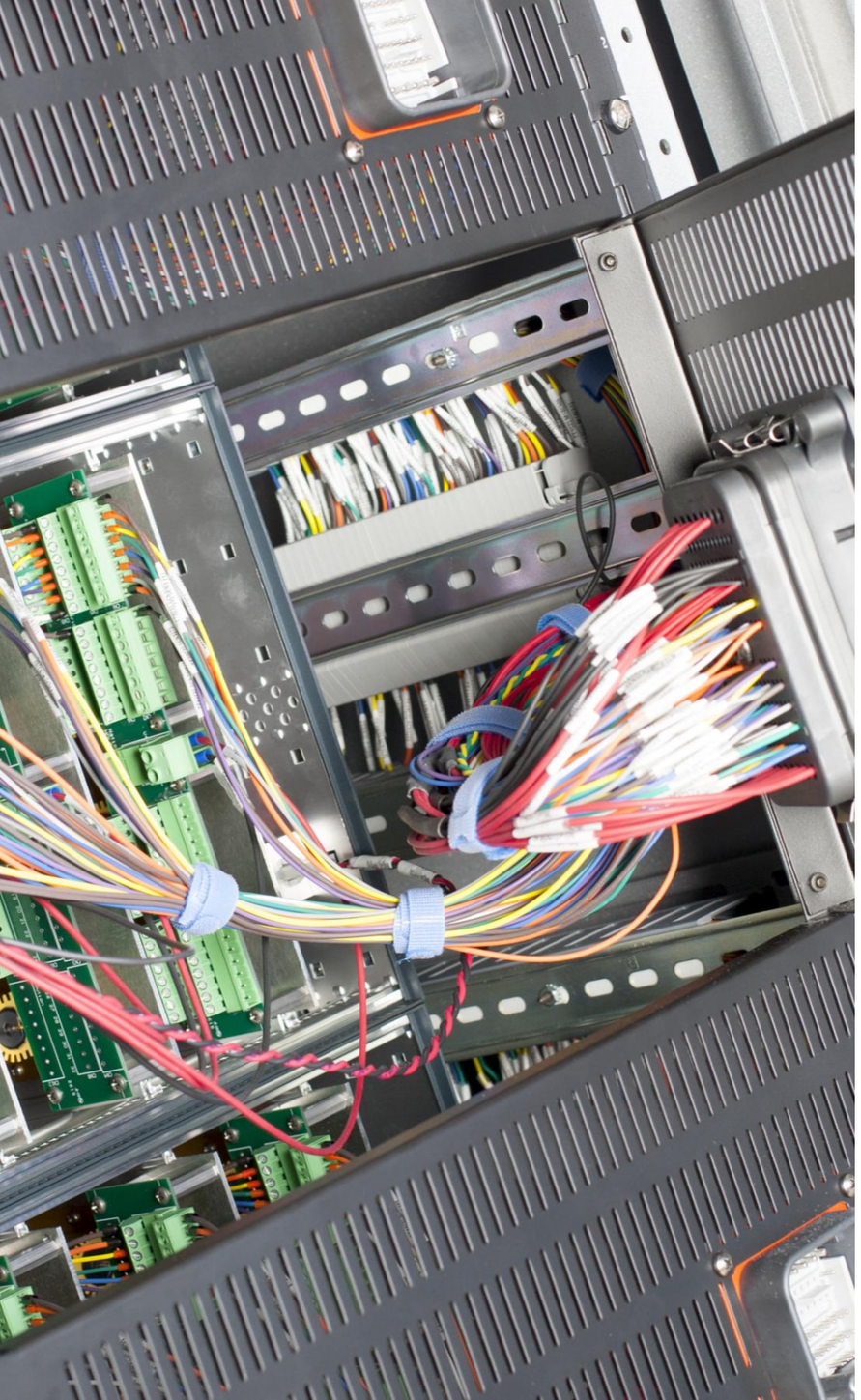
Security Control Questions distributed across SDLC



Government Actions – Overlapping Programs



*Notional - Not to scale



What does this mean for Test?

Your IT team will continue to push security requirements to test systems

- *They need to comply with corporate security mandates*

Projects you deliver to government agencies or contractors will include security requirements

- *Government contracts will include security flow downs*

You will need to provide documentation of your secure development

- *European, US, and customer requirements need documentation for compliance*

These may translate to you as:

Requests for documentation:

- Bill of material / Software bill of materials
- Letters of volatility
- Compliance documents to 800-171 / 800-53
- Compliance to NIST 800-218 (SSDF)
- STIGs

Requests for certification

- FedRAMP for cloud services
- ICD-503 software security
- ISO 27001

Security testing

- Static code analysis
- Dynamic system analysis
- Vulnerability scans
- Penetration testing

Software for Professional Test Workflows

Electronics Validation Test

Characterizing electronic prototypes to ensure quality and performance

Set-up & Configure → Measure & Automate → Analyze & Share

Electronics Production Test

Functional test ensuring manufactured products meet specifications

Set-up & Configure → Measure & Automate → Deploy & Maintain

Electromechanical Validation Test

Characterizing physical prototypes to ensure quality and performance

Build & Customize → Configure → Analyze & Share

Embedded Software Test

Testing deployed software for defects across wide parameter variations

Configure & Map → Test & Bring Up → Automate & Execute

Security is a significant part of each of these workflows

EMERSON | NI

Validation Systems

Electronics Test | Areas of Investment

Accessible Automation

Streamline toolchain for validation use case to speed use and lower barrier to entry

Example features
- Automate interactive measurements
- Connect sequencing inside InstrumentStudio

Open Architectures

Compatibility with 3rd party hardware and software tools

Example features
- Panels and pin maps for 3rd party instruments
- Ease use of .NET, Python, MATLAB, C#

Modern Dev Practices

Improve collaborative tools in LabVIEW+ to ease large, complex application development

Example features
- git integration for LabVIEW and TestStand
- Improve diff and merge to support CI/CD

System Security

Meet regulatory requirements for security and share details of exposures

Example features
- SBOMs and CVEs
- IPv6 support

Measurement Transition

Software tool interoperability to quickly share specifications, measurements, data and results

Example features
- Measurement repository
- Generate compliance data from InstrumentStudio

Production Systems

Electronics Test | Areas of Investment

Modernize UI Building

Update UI controls to provide engaging experience for custom interfaces

Example features
- Multilanguage character support
- Web controls

Open Architectures

Compatibility with 3rd party hardware and software tools

Example features
- Step Types for 3rd party instruments
- Ease use of .NET, Python, MATLAB, C#

Modern Dev Practices

Improve collaborative tools in LabVIEW+ to ease large, complex application development

Example features
- git integration for LabVIEW and TestStand
- Improve diff and merge of LabVIEW code to support CI/CD

System Security

Meet regulatory requirements for security, especially when maintaining long term system deployments

Example features
- SBOMs and CVEs
- Linux deployments

Measurement Transition

Software tool interoperability to quickly share specifications, measurements, data and results

Example features
- Use measurements from a library
- Integration with SystemLink

Validation Systems

Electromechanical Test | Areas of Investment

Accessible Automation

Speed system development with connected applications and easy-to-use sequencing.

Example features
- Connect FlexLogger measurements with automation in LabVIEW or TestStand
- Automate durability tests without programming in FlexLogger

Open Integration

Simplify integration of 3rd party hardware, custom algorithms, and control logic.

Example features
- Improve development and debugging of FlexLogger plugins
- Develop custom measurements in any language

Modern Dev Practices

Improve collaborative tools in LabVIEW+ to ease large, complex application development.

Example features
- git integration for LabVIEW and TestStand
- Improve diff and merge to support CI/CD

System Security

Meet regulatory requirements for security, especially when maintaining long term system deployments.

Example features
- SBOMs and CVEs
- Linux RT Identity and Access Management

Out-of-the-box Measurements

Hardware and software built together to deliver measurements in minutes.

Example features
- FlexLogger Lite included with every DAQ device
- Guided setup, reference material and pin layout accessible directly from the hardware

Validation Systems

Embedded Software Test | Areas of Investment

Bus Configuration

Communicate to your DUT using required communication protocols

Example features
- VCOM Custom device
- Communication bus template
- Custom device scripting APIs

Simulink and Model Integration

Integrate models to provide simulated data to your DUT

Example features
- Expanded Simulink™ HDL Coder support for NI Hardware
- FMI 3.0 Support

Debugging

Improve tools to quickly identify & resolve errors when building your HIL system

Example features
- Improved custom device debugging
- Error handling, diagnostics, and debugging with in VeriStand

System Security

Meet regulatory requirements for security, especially when maintaining long term system deployments

Example features
- SBOMs and CVEs
- Linux deployments

Accessible Automation

Increase test throughput by automating the HIL test system

Example features
- VeriStand steps for TestStand
- In-product sequencing

“…most attacks exploit persistent vulnerabilities such as outdated software…”

“For control systems, it is much easier to penetrate and compromise critical infrastructures as there is little to no cyber security in control system field devices and no cyber security training to address these issues.”

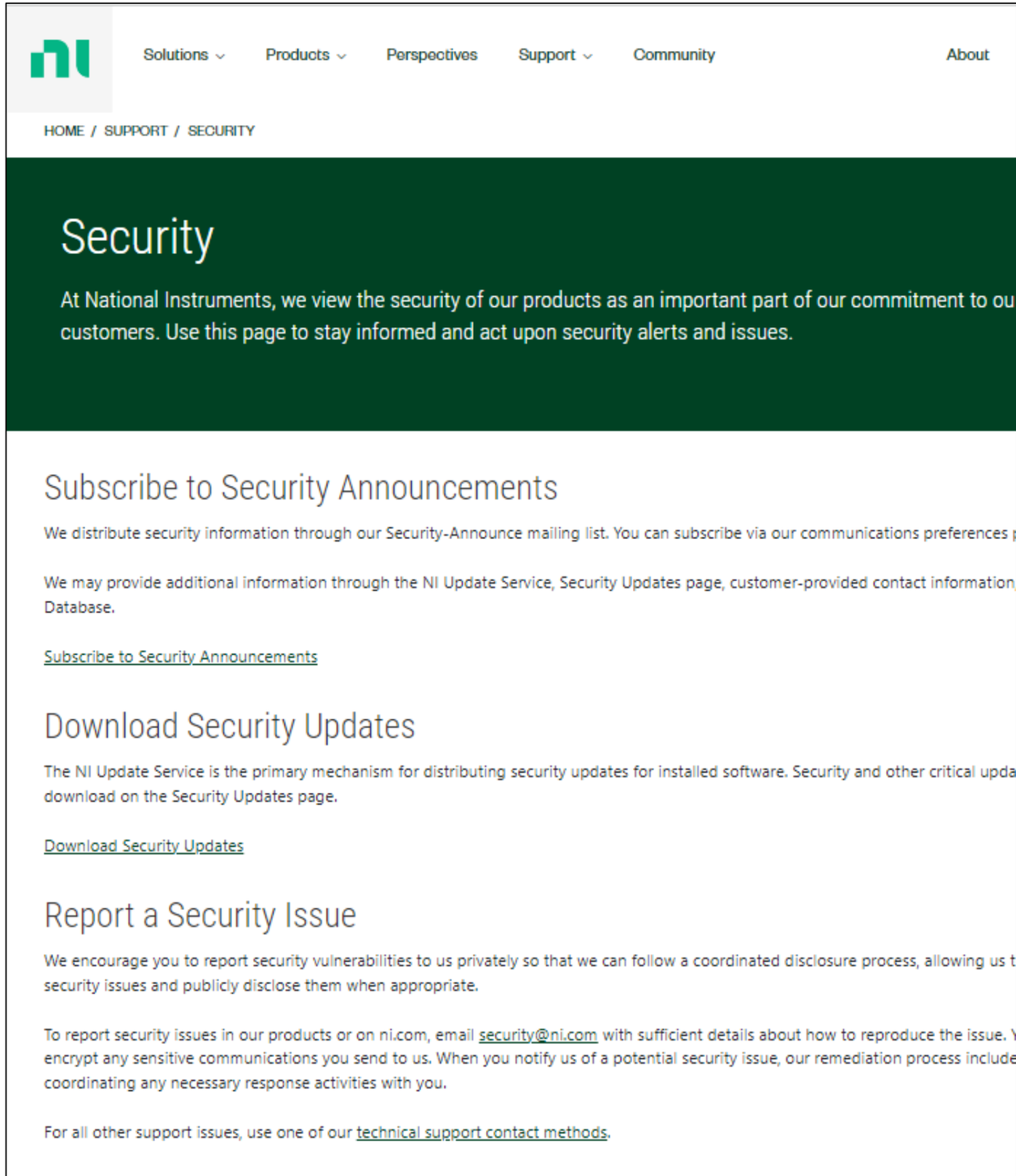
Software Updates

The way test systems are funded and maintained for is not a model that supports ongoing security.

- Steve Summers

NI Resources for security

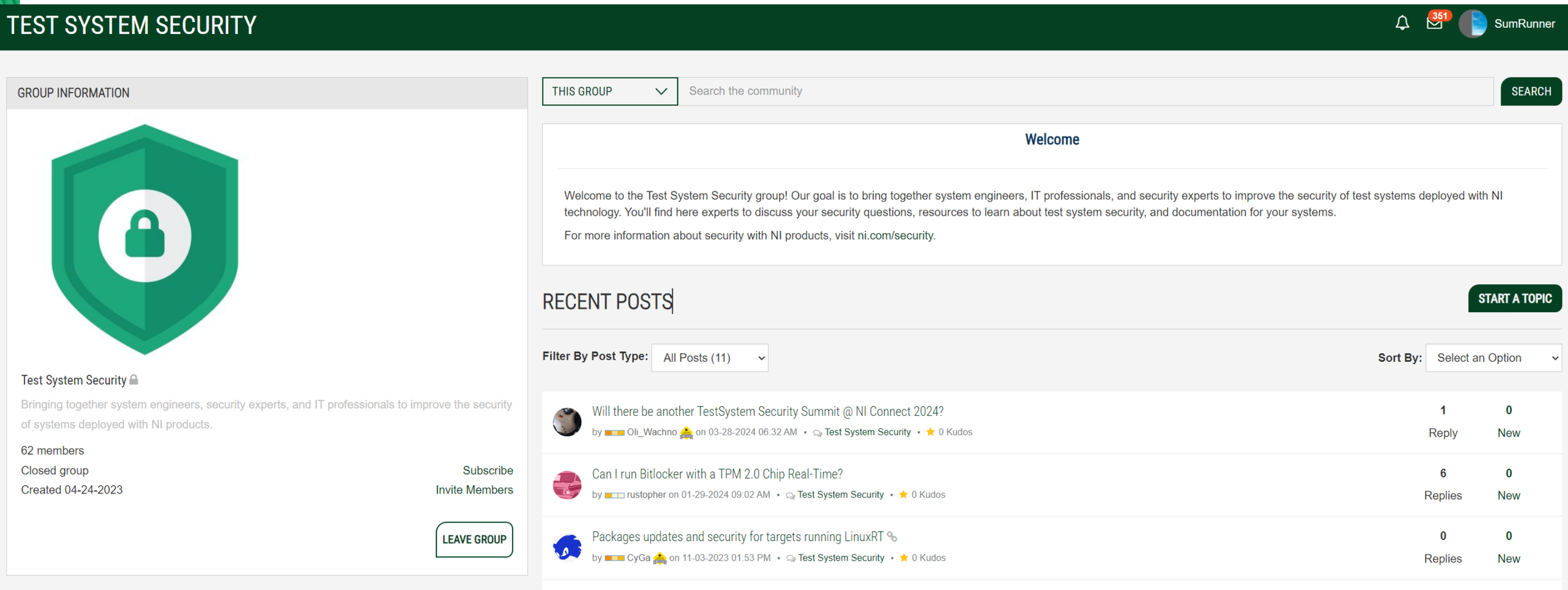
- **ni.com/security** – first stop for security information
- **security@ni.com** – report issues, request information
- **Letters of volatility** – with product manuals or at ni.com/letters-of-volatility
- **Secure development guides** – at ni.com/security
- **Additional security documentation** – available on request



Test System Security Forum

- Online Forum – Join for access
- Next meeting (virtual) – June 18 2024

  Join forum to receive invites



NI Test System Security Summit

Semi-annual meeting for test engineers, security teams, and IT professionals

Online forum to access discussions, presentations

Next meeting: June 18 2024

To be invited:

Email steve.summers@ni.com


This is a journey

security@ni.com
ni.com/security
steve.summers@ni.com
kyle.tetmeyer@ni.com

CONNECT