Center for Internet Security (CIS) Benchmark for Liberty

Ajay Reddy
Senior Software Engineer
IBM WebSphere Security

Department of Defense Security Standards (STIG)

Emily Tuczkowski
Senior Software Engineer
IBM WebSphere Security
Security Compliance Focal

September 14th 2022

Agenda

- Introduction to Center for Internet Security (CIS)
- Deep dive into the CIS Liberty recommendations.
- Introduction to Security Technical Implementation Guide (STIG)
- Deep dive into STIG for WebSphere.

Introduction to CIS

- Goal
  - Make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.
  - Leading the global community to secure our ever-changing connected world.
- How
  - Bringing together a global community of cybersecurity experts to develop proven and effective, consensus based, best practices to help secure everything from your home laptop and mobile phone, to the networks and applications that run the largest companies on earth.
  - Providing CIS Controls and Benchmarks at no-cost for anyone to use.

CIS Controls and Benchmarks

- The CIS Critical Security Controls (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks.
  - https://learn.cisecurity.org/cis-controls-download
  - https://workbench.cisecurity.org/benchmarks/6480
- They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. CIS Controls v8 has been enhanced to keep up with modern systems and software.
  - Example:

    3.10 Encrypt Sensitive Data in Transit

    Description

    Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

CIS Benchmarks

- A CIS Benchmark describes consensus best practices for the secure configuration of a target system.
  - For example: Liberty, Red Hat OpenShift
- All CIS Benchmarks contain individual security recommendations that may contain the various sections in the table

- Title
- Assessment Status
- Profiles
- Description
- Rationale Statement
- Audit Procedure
- Remediation Procedure
- Impact Statement
- Default Value
- CIS Controls
- References
- Additional Information

CIS usage and tools

- CIS creates/supports CIS Benchmarks in the multiple formats like Word, PDF, Excel
  - The PDF versions are available for free on www.cisecurity.org
- Automated Assessment Content (AAC)
  - AAC via CIS-CAT (Configuration Assessment Tool) Pro with CIS SecureSuite Membership
  - CIS-CAT automatically compares a target system's configuration settings to recommended settings in more than 80 CIS Benchmarks.
    - https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro_pre
  - Confirm to the NIST (National Institute of Standards and Technology)'s SCAP (Security Content Automation Protocol) specification.
- 3rd party vendors also integrate CIS Benchmarks into their tools
  - Examples: Tenable, Qualys
- One can write their own tools to verify these recommendations.

Links

- www.cisecurity.org
- https://www.cisecurity.org/benchmark/websphere
  - WAS Liberty recommendations PDF download
- https://workbench.cisecurity.org/benchmarks/7724
  - WAS Liberty benchmarks
  - Requires a (free) account setup
- https://www.cisecurity.org/cybersecurity-tools/mapping-compliance
  - CIS controls mapping to additional security frameworks

Liberty CIS Benchmarks Demo

Department of Defense Security Standards: STIG

Getting the Right Protections in Place

Department of Defense: Security Standards

- In order for IBM to sell our products to the Department of Defense (DoD)and its subsidiary agencies, we must prove that our offerings fulfill a set of security compliance standards.
- The DoD is an executive branch department of the federal government charged with coordinating and supervising all agencies and functions of the government directly related to national security and the United States Armed Forces. Security is CRITICAL.
- Those standards are defined by an organization, an intermediary between IBM and the DoD, called DISA, or the Defense Information Systems Agency.

Department of Defense: Security Standards

- DISA responsibilities include:
  - Developing and maintaining Security Requirements Guides (SRGs) and Security Technical Implementation Guides (STIGs)
  - Providing guidance used in Command Cyber Readiness Inspection (CCRIs) and certification and accreditation (C&A) activities (compliance) as well as vendor product development
  - Developing and disseminating operationally implementable secure configuration Guidance for use throughout the DoD
  - Serving as the Information Systems Security Manager (ISSM) for the Risk Management Executive (RME) and Operations Center (OPC)

Department of Defense: Security Standards

- These objectives:
  - Securing shared information environments
  - Ensuring the classified capability of mobile data
  - Secured transactions in the Cloud
  - Secure networks
  - …. and more
- Are met by the STIG

What is the STIG

- Security Technical Implementation Guide
  - An operationally implementable compendium of DoD controls, security regulations, and best practices for securing an operating system, network, application software, etc.
  - Providing guidance for areas including mitigating insider threats, containing applications, preventing lateral movements, and securing information system credentials
- Goals
  - Intrusion Avoidance
  - Intrusion Detection
  - Response and Recovery

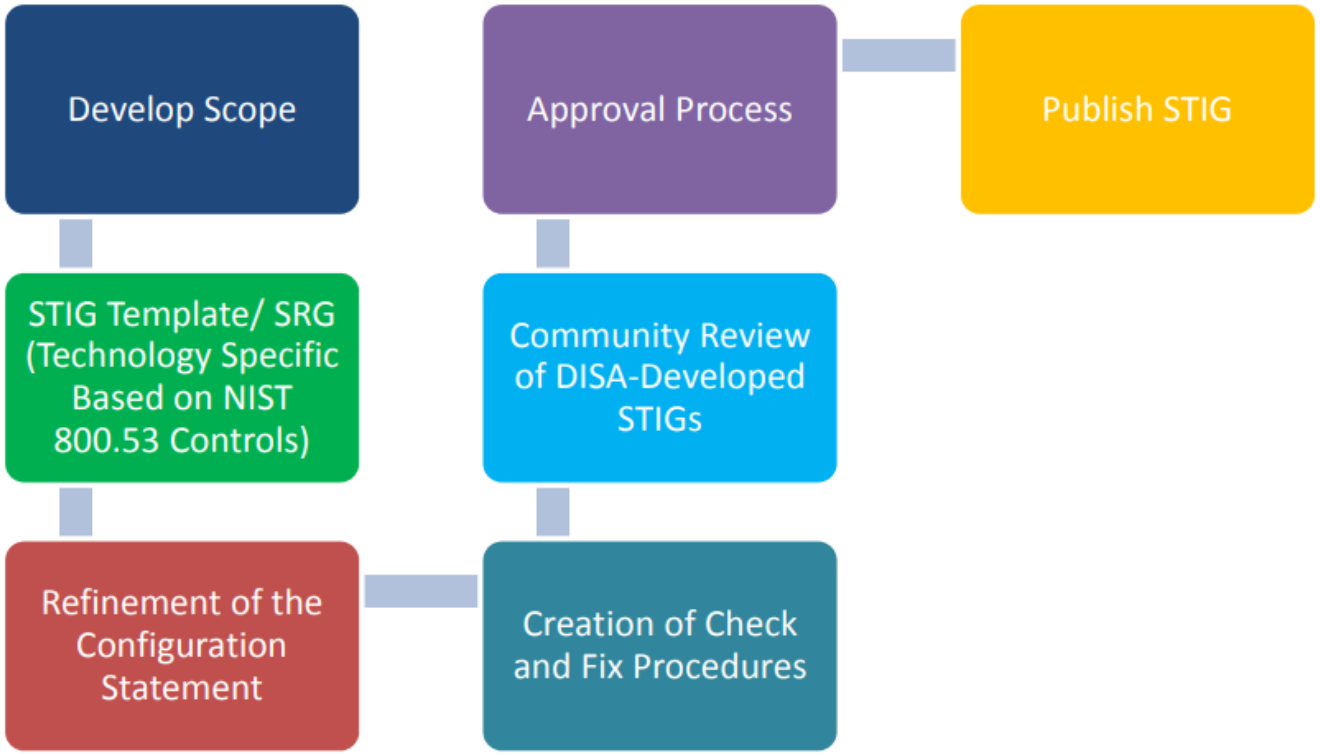
Why is the STIG important to our customers

- STIGs are the source of configuration guidance for network devices, software, databases and operating systems. The aim is to lower the risk of cybersecurity threats, breaches and intrusion by making the set-up of the network as secure as possible.
- If you are providing an application, networking interface or any functionality to the DoD which sits on top of either Traditional WebSphere or Liberty, you have the assurance that our underlying application server is STIG compliant.
- By using our security functionality, you can be assured that mechanisms are in place to ensure the integrity of the environment, making it inherently secure.
- And that opens up the door to your being able to sell your products to the DoD.

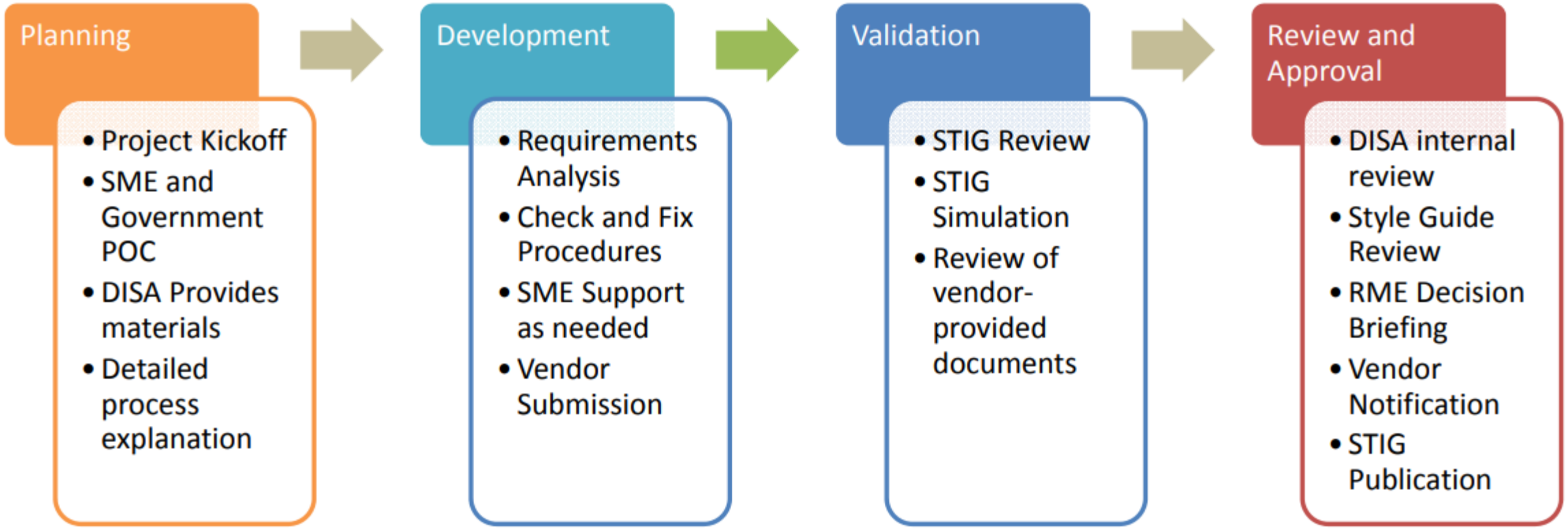
STIG Impact Statement

- Internal analysis has shown over 96% of cyber incidents could have been prevented if STIGS were applied
- Rapid response to real-time cyber attacks
- Industry and government can benefit from security standards

STIG Development Process



Vendor STIG Process



Reaching Approval

- **Participants include:**
  - **DoD Services and Agencies**
  - **Federal Agencies**
  - **NSA**
  - **Vendors**

Where do I find our IBM-approved and other STIGs

- There are over 16,000 registered users
- Over 920,000 hits per month
- Support for users questions in excess of 3000 each year

http://iase.disa.mil/stigs/index.html

Go Here

Demo: Liberty WebSphere input into STIG

Call-to-Actions Charts for Engagement

Open Liberty

Useful Links

Why choose Liberty for Microservices
https://ibm.biz/6ReasonsWhyLiberty

Choosing the right Java runtime
https://ibm.biz/ChooseJavaRuntime

How to approach application modernization
https://ibm.biz/ModernizeJavaApps

Open Liberty Site
https://www.openliberty.io

Open Liberty Guides
https://www.openliberty.io/guides

https://openliberty.io →

Join the WAS CAB

WebSphere Customer Advisory Board

Email:
claudiab@us.ibm.com

Webex:
https://ibm.webex.com/meet/claudiab

Community Resource:
http://ibm.biz/WASCABCommunityResources

Advisory Board:
http://ibm.biz/WebSphereAdvisoryBoard

Weekly meetings

Thursday and Friday
9:15 am EST

Join →

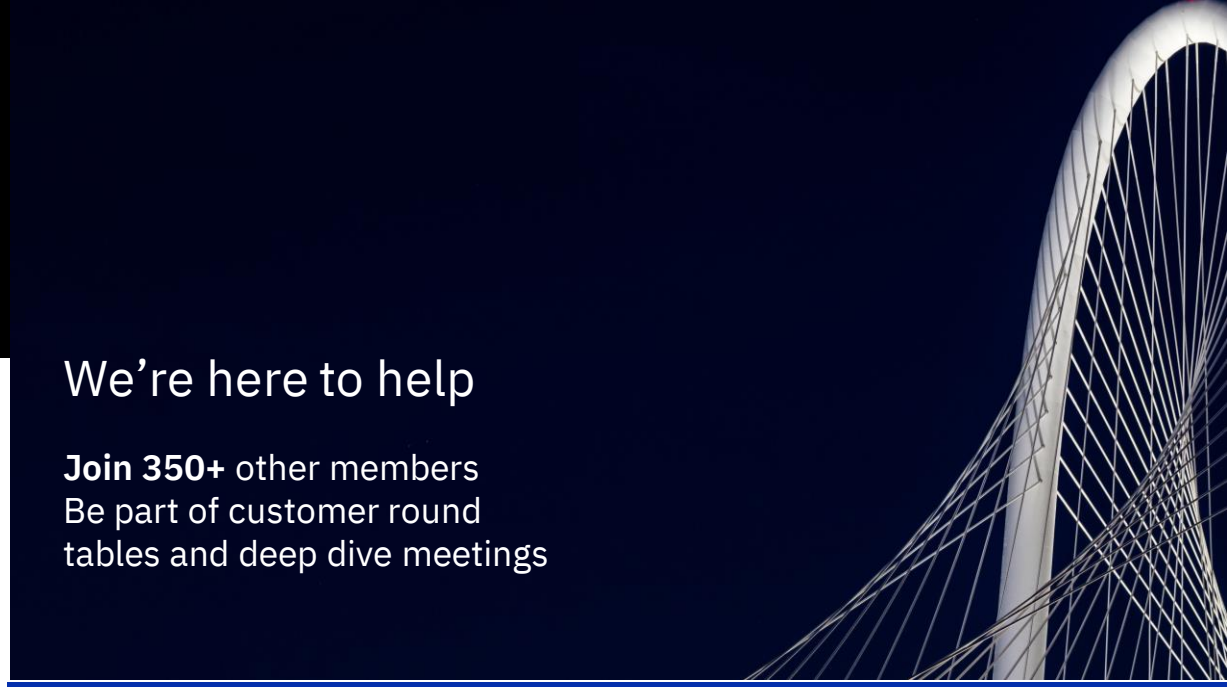
Monthly meetings

- Business Partner track
- Time zone friendly sessions

Join →

Other Programs

- Cloud Pak Week
- Previews, Demos
- Labs, workshops
- 1-on-1



We're here to help

Join 350+ other members
Be part of customer round tables and deep dive meetings

Engage when you have time:

- Stay in the loop at meetings
- Share solutions and pain points
- Connect with other customers
- Access to resources and experts
- Customized meetings
- Special offers