Communication ISAC International Symposium on Cybersecurity, Tokyo, Japan November 11, 2019

Joe Viens, Sr. Director Government Affairs, Charter Communications

Chair, Communications Information Sharing and Analysis Center

Secretary, National Council of isac's

Communications Sector Coordinating Council, Executive Committee

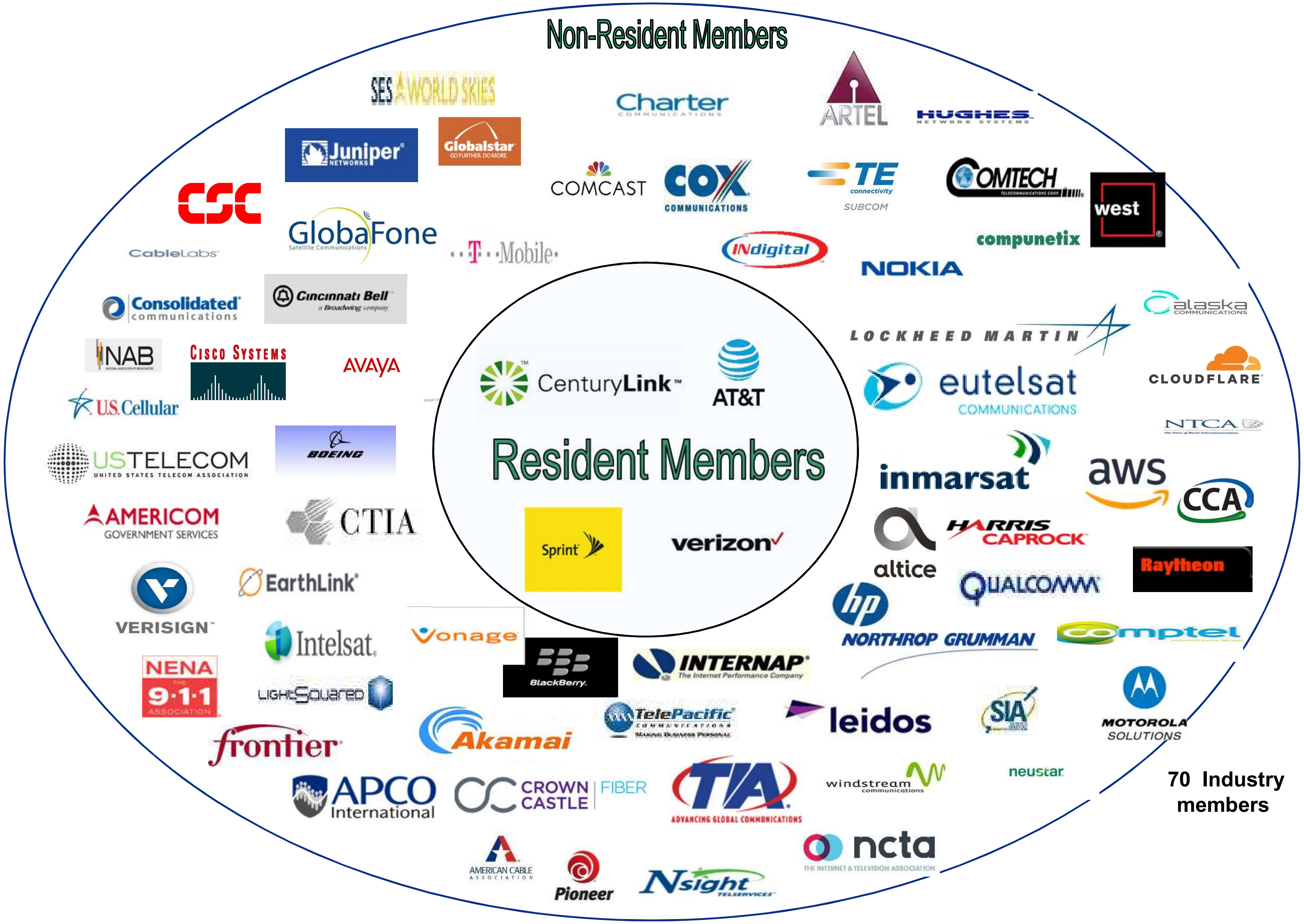
Background

- All Hazards Public/Private Partnership 35+ Years – Department of Homeland Security – Cybersecurity and Infrastructure Security Agency (CISA) – CISA Integration Operations Coordination Center – National Communications Coordination Branch – CIOCC/NCC.
- 70 Industry Members – Network Service Providers, Associations, Communication Hardware Suppliers, and Other Communications Related Industry. 99%+ of Industry Represented.
- Government Agency Members – Department of Homeland Security/CISA/FEMA, Federal Communications Commission, Department of Treasury, Department of Defense, Department of State, Department of Energy and others.
- NCC-COMM ISAC Primary Mission – National Security/Emergency Preparedness
  - Continuity of Communications for USA

Operationally Focused Information Sharing

- DHS/CISA CIOCC/NCC - 24/7 Watch
- Joint Meeting every Monday Morning 0900
- Network Service Providers Meet Every Monday Morning 1000
- Come together during significant events: Natural - Hurricanes, Wildfires, Earthquakes,….etc. Man Made - Cyber Related Events, Terrorism, Protests, ….etc.
- National Security Special Events: Superbowl, Inauguration, Olympics, Political Conventions, Pope Visit…….etc.
- National Level Exercises – CyberStorm, New Madrid, Cascadia Subduction Zone, …….etc.

NCC Communications ISAC Industry Members



Non-Resident Members

Resident Members

70 Industry members

Communications ISAC Initiatives

- 2020 National Level Exercise Planning
  - CyberStorm 2020
- Tri-Sector Collaboration – Communications, Finance, and Electric
  - Playbooks
  - Exercises
  - Come together during significant events
- Communications/Electric Collaboration
  - Debris Removal
  - Cut Fiber
  - Prioritization of Restoral
  - REMEMBER THERE IS NO CYBER WITHOUT FIBER
- Information and Communications Technology Supply Chain Risk Management Taskforce
- DNS/BGP Working Group
- IOT Certification

Information and Communications Technology Supply Chain Risk Management Task Force

Presentation to International Symposium on Cybersecurity

November 11, 2019

Agenda Items

- Introductions and Overview of Meeting Agenda
- Definition of C-SCRM and Prerequisite Work
- ICT SCRM Task Force Working Group Descriptions
- Questions & Closing Remarks

Definition and Prerequisite Work

Definitions

NIST definition: ***Cyber Supply Chain Risk Management (C-SCRM)*** *is the process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of ICT product and service supply chains. C-SCRM covers the entire life cycle of ICT.*[1]

- Encompasses hardware, software, and information assurance, along with traditional supply chain management and supply chain security practices.

[1] See, NIST definition of C-SCRM, available at: https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management. For purposes of the ICT SCRM Task Force, the term "ICT" includes operational technology and "Internet of Things" devices and services.

Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Subchap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018)
"*Covered articles*" means:

- Information technology, including cloud computing services of all types (41 USC 4713(k)(2)(A));
- Telecommunications equipment or telecommunications service (41 USC 4713(k)(2)(B));
- The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (41 USC 4713(k)(2)(C));
- All IoT/OT – (hardware, systems, devices, software, or services that include embedded or incidental information technology). (41 USC 4713(k)(2)(D))

Federal Supply Chain Inventory

Objective: Collect and analyze existing and planned ICT C-SCRM initiatives across Federal Government, best practices, and standards in order to better understand the current landscape of existing activities.

Approach:

- DHS has developed a Data Matrix to capture Agency's ongoing or planned activities
- Data call will be sent to Federal Agencies by OMB
- Analyze and compile data call results
  - Share with industry WG members
- Draft deliverable and plan for Government use
- Deliver compiled information in a "living" document that will be integrated with the Industry Inventory results as input for the other ICT Task Force Working Groups (primarily, Threat Assessment and Qualified Bidders List/Qualified Manufacturers List)

Industry Supply Chain Inventory

Objective: Compile an inventory of industry best practices addressing supply chain risk management.

Approach:

- Inventory SCRM standards and guidance activities used in Industry
- Annotate identified inventory of standards with descriptive information including reference materials
- Provide example "Use Cases" from industry application of SCRM standards
- Identify organizations that develop, contribute, track SCRM standards
- Finalize content and draft deliverable
- Deliver compiled information in a "living" document that will be integrated with the Government Inventory results as input for the other ICT Task Force Working Groups (primarily, Threat Assessment and Qualified Bidders List/Qualified Manufacturers List)

ICT C-SCRM Task Force Working Group Descriptions

Working Group #1: Information Sharing WG Overview

Work Group 1 Description:

- Development of a common framework for the bi-directional sharing of supply chain risk information between government and industry

Objective:

- WG1 seeks to define the scope of its efforts by reviewing/discussing risks and a synthesized agreed upon cyber supply chain risk management definition leading toward the development of a common framework for information sharing

Working Group #2: Threat Evaluation WG Overview

Working Group 2 Description:

- Identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services.

Objective:

- Produce a set of processes and criteria for conducting supplier, product, and service threat assessments.
- The processes and criteria will initially be focused only on global ICT supplier selection, pedigree, and provenance. It will also address product assurance (hardware, software, firmware, etc.), data security, and supply chain risks.
- Finally, the process and criteria will establish a framework for a threat based assessment of cyber supply chain risks that can be extended in future work products to address other critical infrastructure sectors.

Working Group #3: Qualified Bidder/Manufacturer Lists WG Overview

Working Group 3 Description:

- Identification of market segment(s) and evaluation criteria for Qualified Bidder Lists and Qualified Manufacture Lists (QBL/QML).

Objective:

- Determine a foundational scope for the Working Group. Identification and Prioritization of Objectives/Goals, Deliverables, Timelines, Methods for Information Sharing, Reporting Requirements/Primary/Secondary Points of Contact, Meeting Schedules, Resources, and Risks.

Working Group #4: OEM & Authorized Resellers WG Overview

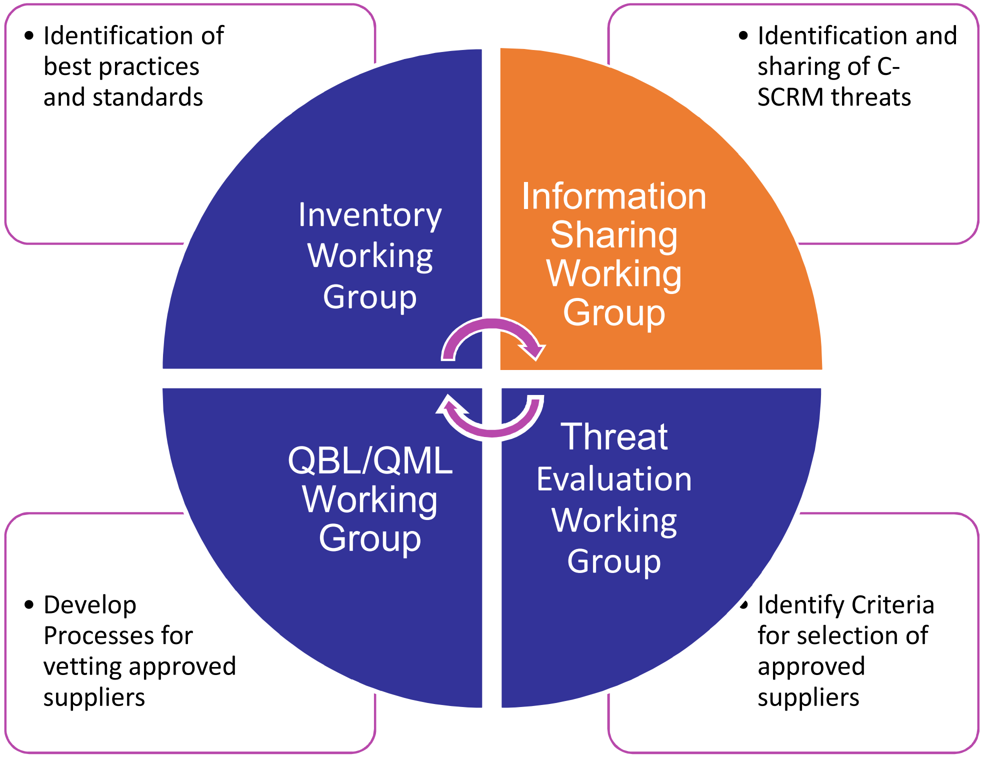
Working Group 4 Description:

- Produce a policy recommendation(s) to incentivize the purchase of Information and Communications Technology (ICT) products—hardware; software; devices; and systems—from original equipment manufacturers or authorized resellers.

Objective:

- Achieve consensus between Government and Industry Working Group members for a realistic, practicable, and executable policy recommendation(s) that will meet the needs of both government and industry procurement professionals.

Collaborative C-SCRM Task Force Work Flow



- Identification of best practices and standards

- Identification and sharing of C-SCRM threats

- Develop Processes for vetting approved suppliers

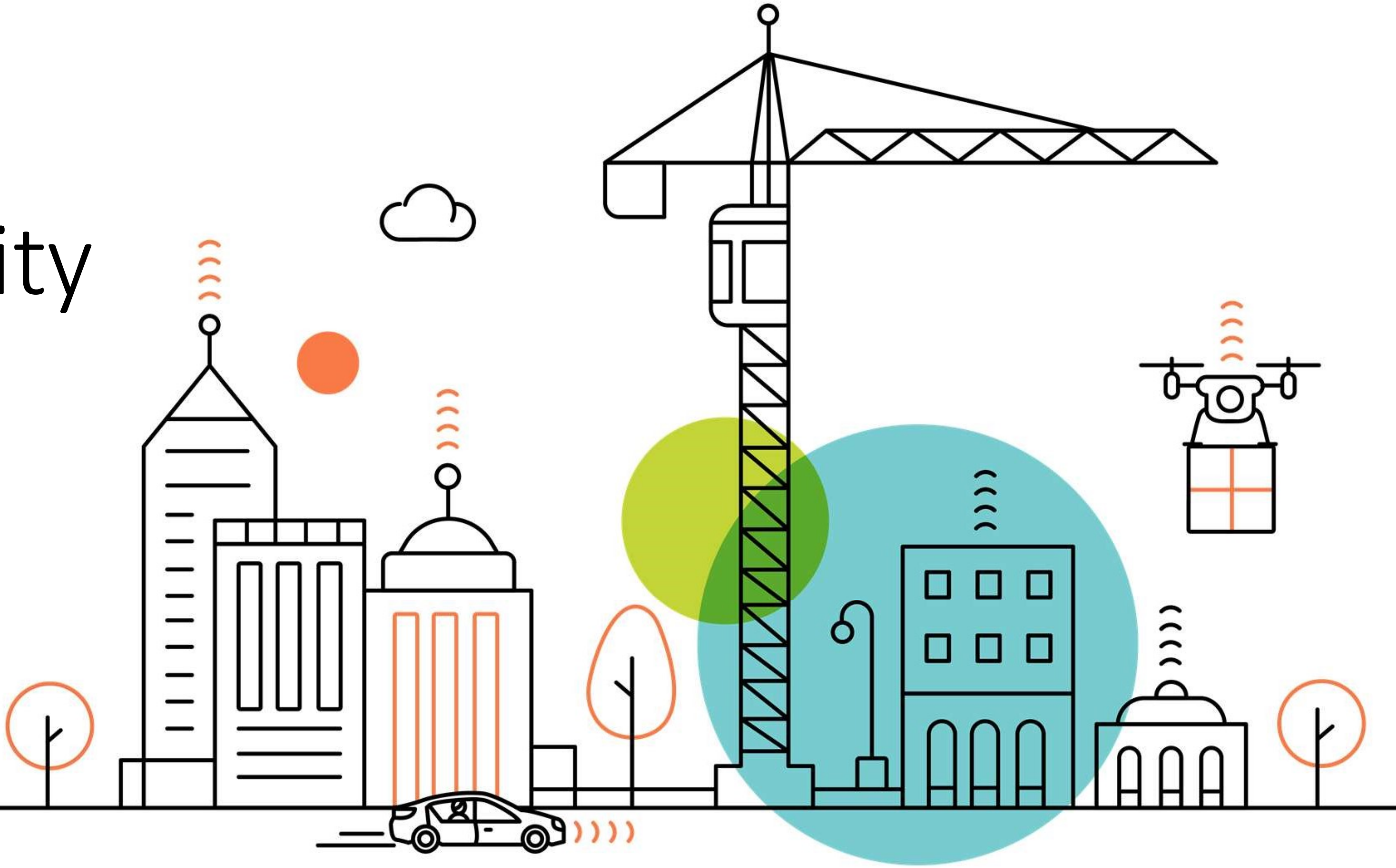
- Identify Criteria for selection of approved suppliers

Inventory Working Group
Information Sharing Working Group
QBL/QML Working Group
Threat Evaluation Working Group

IoT Cybersecurity Certification

November 11, 2019

Drew Morin



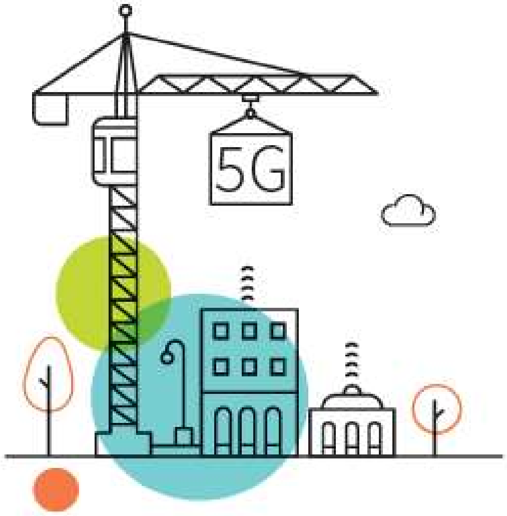
New CTIA Cybersecurity Certification Program

Cybersecurity for Devices on Wireless Networks

This program was developed with the support of wireless operators with the goal of voluntarily establishing device cybersecurity best practices in the wireless industry. This is the first mobile device cybersecurity program of its kind to have the backing of wireless operators in collaboration with technology companies and certification test labs.

The Cybersecurity Certification Program:

- Certifies security elements of LTE and 5G devices, including those with Wi-Fi connections
- Creates an industry best practice for IoT security on wireless networks
- Helps protect consumers and wireless infrastructure, while creating a more secure foundation for smart cities, connected cars, mHealth, and other IoT applications



Potential Cybersecurity Government Initiatives

US Federal Bills

- Internet of Things (IoT) Cybersecurity Improvement Act of 2019 (minimum standards for Fed acquired IoT)
- Cyber Shield Act of 2017
- Security IoT Act (minimum standards for IoT and FCC enforcement)

US State Bills

- California: IoT Cybersecurity Improvement Act of 2017
- Maryland: The Internet of Things (IoT) Cybersecurity Improvement Act of 2019
- Illinois: The Internet of Things Improvement Act
- Kentucky: The IoT Cybersecurity Improvement Act

EU ENISA: Cybersecurity Act (CSA)

UK Code of Practice

Protecting Wireless Networks

The IoT Cybersecurity Certification Program Working Group convenes wireless operators, OEMs and laboratories:

Create cyber best practices

Identify cyber risks and establish industry test plans

Educate consumers

Create industry and consumer awareness

Work with policymakers

Champion policy initiatives to combat cyber threats

Build security tools

Certification programs set criteria and minimum requirements

Developing a Cybersecurity Baseline

IoT Cybersecurity Certification uses three levels, depending on the sophistication of device and security characteristics needed, to develop a baseline set of cybersecurity criteria:

Level 1

Core security meets the needs of consumer-grade devices.

Elements Include:

- Terms of Service & Privacy Policy
- Password Management
- Authentication Test
- Access Controls
- Patch Management
- Software Upgrades

Level 2

Enhanced security is well-suited for business and enterprise-managed devices.

Elements Include:

- Includes level 1 elements
- Audit Log
- Encryption of Data in Transit
- Multi-Factor Authentication
- Remote Deactivation
- Secure Boot
- Threat Monitoring
- IoT Device Identity

Level 3

Advanced security offers features designed to protect infrastructure-managed devices.

Elements Include:

- Includes level 2 elements
- Digital Signature Generation and Validation
- Encryption of Data at Rest
- Tamper Resistance
- Design-In Features

IoT Cybersecurity Certification Program in Action

Eight authorized CTIA Cybersecurity Certification test labs to-date

- 7Layers (Irvine, CA)
- Ericsson (Richardson, TX)
- Intertek (Lexington, KY)
- Intertek (Rockville, MD)

- PCTEST (Columbia, MD)
- SGS (San Diego, CA)
- Spirent (San Jose, CA)
- UL (Fremont, CA)

Press Release

CTIA IoT Cybersecurity Certification Program Certifies First Device

- March 7, 2019: HARMAN Spark, offered at AT&T, tested by Ericsson

Program Documentation

Cybersecurity Certification Test Plan for IoT Devices

ctia.org/about-ctia/test-plans/

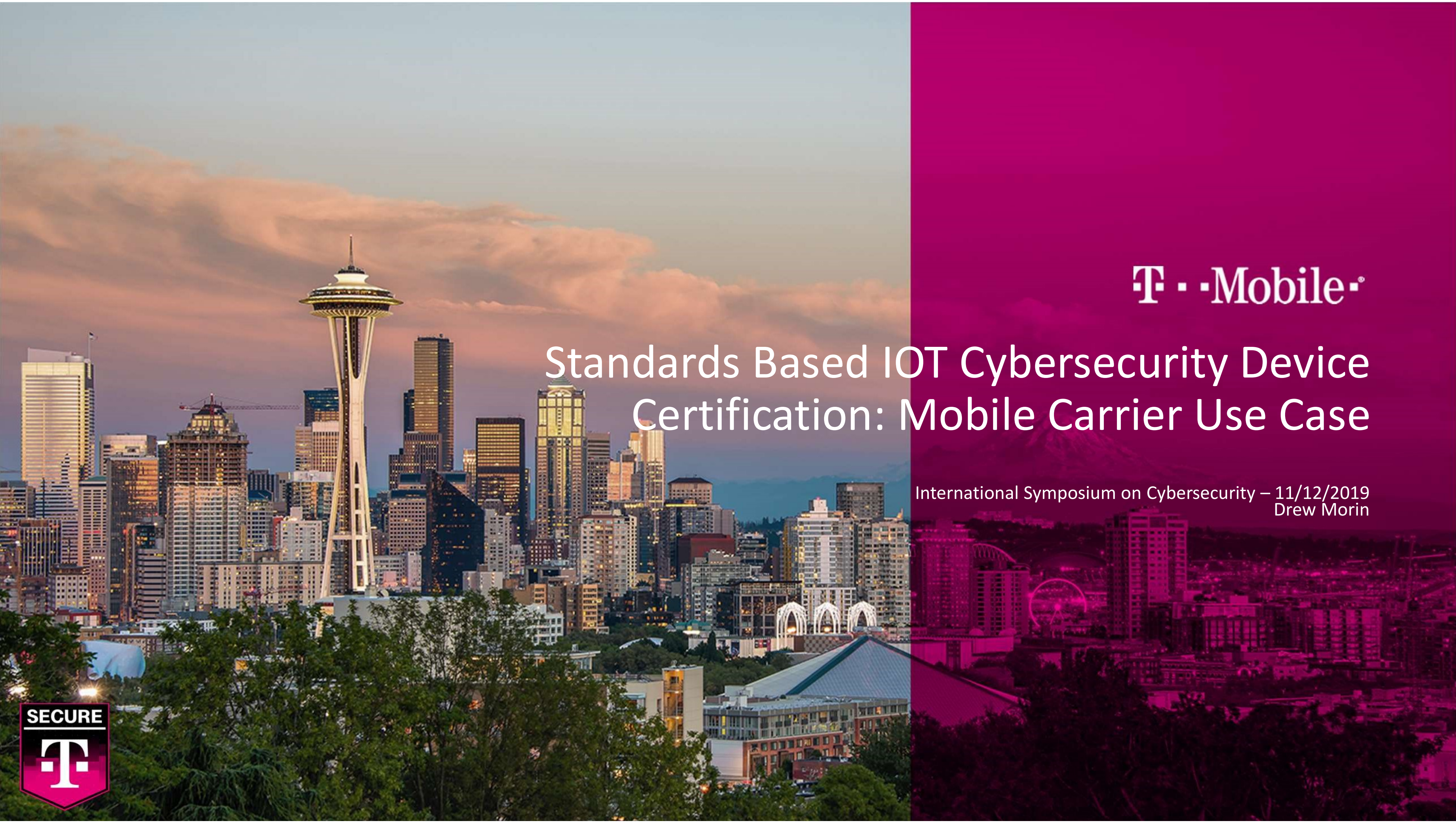
IoT Cybersecurity Certification Program Management Document and Vendor Questionnaire

https://api.ctia.org/wp-content/uploads/2019/05/ctia_IoT_cybersecurity_pmd_ver-1_1.pdf

- Questionnaire can help a vendor or CATL to determine the device readiness for testing at each level.

CTIA Certification

certification@ctiacertification.org



Standards Based IOT Cybersecurity Device Certification: Mobile Carrier Use Case

International Symposium on Cybersecurity – 11/12/2019
Drew Morin

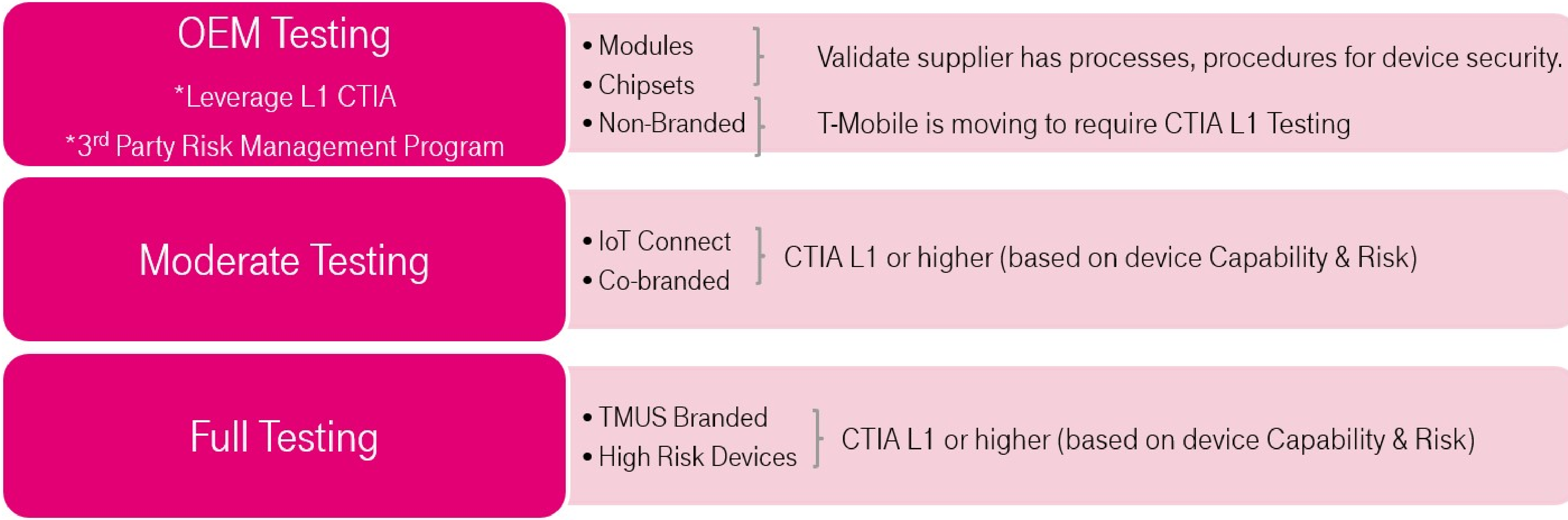
Shift Security Left | Security By Design

- Partner with key Industry leaders to drive Standards
- Require progressive security requirements for T-Mobile devices
- Validate & Enforce Key Security Requirements
- Partner with OEMs/Service Providers to ensure Device Security is a high priority
- Security Patent Effort

What We test Today

***CTIA Testing is based on Capability & Risk**

T-Mobile Device Testing



OEM Testing *Leverage L1 CTIA *3rd Party Risk Management Program	• Modules • Chipsets • Non-Branded	Validate supplier has processes, procedures for device security. T-Mobile is moving to require CTIA L1 Testing
Moderate Testing	• IoT Connect • Co-branded	CTIA L1 or higher (based on device Capability & Risk)
Full Testing	• TMUS Branded • High Risk Devices	CTIA L1 or higher (based on device Capability & Risk)

Security Testing Overview

Device

Physical

Review + Validate HW Security
Debug Port Testing
Flash Memory Protection Testing

Network

Scanning open ports/services
Identifying possible exploits for listening services
Exploit custom logic, custom API's, webpages, etc
Capture, Analysis, and Fuzzing/Manipulation of network traffic
Validate HTTPs connections properly validate

Firmware

Validate signing and other FW protections
Validate authenticated FW update procedure
Analysis of included binaries/scripts/tools/fw images

*Only highlighted items are included in Medium Level Testing.
All items included in Full Level Testing

Application

Design

Review + Validate application architecture

Code

Disassembly and analysis of application

Network

Capture, analysis, and fuzzing/manipulation of network traffic
Validate that HTTPS connections properly validate certificates

Cloud

Design

Review + Validate cloud architecture

Network

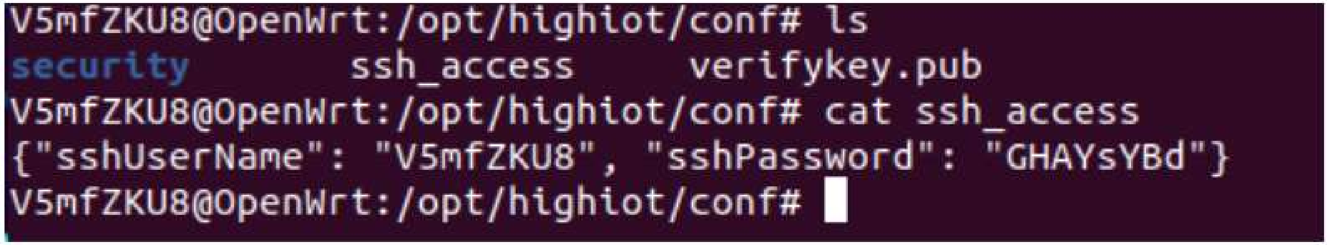
Scanning open ports/services
Scanning for exploits targeting listening services
Validate that HTTPS connections properly validate certificates
Enumerate DNS domains to discover additional servers/services
Capture, analysis, and fuzzing/manipulation of network traffic

Service

Validate proper authentication and authorization is being required for all calls
Injection of malicious network traffic in attempt to trigger vulnerabilities

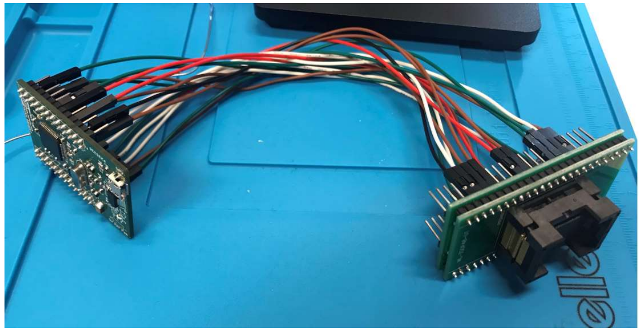
Device – Physical Security

- Goal: Find ways to exploit the software via HW vulnerabilities
- Review + Validate HW Security
  - **Debug Port Testing**
    - Ensuring debug ports are disabled/exploit open ports
    - UART Recovery Mode tests etc.
- Flash Memory Protection Testing
  - Dump from Flash memory/Write to Flash Memory



```
V5mfZKU8@OpenWrt:/opt/highiot/conf# ls
security        ssh_access      verifykey.pub
V5mfZKU8@OpenWrt:/opt/highiot/conf# cat ssh_access
{"sshUserName": "V5mfZKU8", "sshPassword": "GHAYsYBd"}
V5mfZKU8@OpenWrt:/opt/highiot/conf# 
```

Ex. Dumping secrets (SSH credentials) through firmware dump



Setup to dump TSOP48 NAND flash to recover FW from device

Device – Network Interface

- Scanning open ports/services (ex. OEM originating open ports)
- Identifying possible exploits for listening services
  - Exploit custom logic, custom API's, webpages, etc.
- Capture, Analysis, and Fuzzing/Manipulation of network traffic
  - Leverage Network Analysis tools
- Ensure HTTPS connections properly validate

Device – Firmware

- Validate signing and other FW protections
  - Using Secure Boot, TEE etc.
- Validate authenticated FW update procedure
- Including analysis of on-device:
  - Binaries
  - Scripts
  - Firmware images

Device Application Software

- *Design*
  - Review + Validate application architecture
- *Code*
  - Disassembly and analysis of application (also helpful for maliciously infected devices from the factory that contact “Command & Control”)
  - Review source code (when available)
- *Application Network Traffic*
  - Capture, analysis, and fuzzing/manipulation of network traffic
  - Validate that HTTPS connections properly validate certificates

Cloud Services

- *Design*
  - Review + Validate cloud architecture

- *Network*
  - Scanning open ports/services for the Cloud Service
  - Identifying known exploits targeting listening services
  - Reconnaissance effort to find additional unadvertised servers attached to the service

- *Service Specific Security Tests*
  - Validate proper authentication and authorization is being required for all calls
  - Injection of malicious network traffic in attempt to trigger vulnerabilities