IOT DEVICES WITHIN BUSINESS/HOME ENVIRONMENT

by Matthew Coleman, Cyber Security Engineer & Carl Copeland, Senior Network & Solutions Architect

SECTION 1) INTRODUCTION

As devices continue to develop wireless and internet capabilities, the internet of things (IOT) becomes dense with new endpoints. These devices and access points range in security strength, leaving many vulnerable. Threat actors are not ignorant to this trend, in fact they are in favor of it. Cybercriminals are on the cutting edge of tools used to breach networks and have reached the point of automation with these attacks. These factors led to IOT devices having a 32.72% rate of infection across all platforms in 2020, nearly doubling the stat from 2019. The bottom line is the more devices visible on the internet, the more infections that will occur. Negligence to the state of the current cybersecurity climate will only magnify these results. Preparedness is the best response to a security threat; most organizations have wireless devices but are not ready to deal with a threat actor. To evaluate how this information could affect your organization consider questions like: where are your facilities wireless boundaries? What could an adversary want from you? Security makes use of borders, gates, fences and walls; are yours as seamless digitally as they are physically?

This report addresses a range of cybersecurity risks posed by emerging non-terrestrial based, wireless communications platforms. Cyber threat vectors made entirely out of code and leveraging operational technology security vulnerabilities have been targeting industrial automation and control systems (IACS) since the open release of STUXNET in 2010. Now with the dramatic growth of wireless devices, those threat vectors can be introduced with ease and at scale to critical infrastructure plants in the U.S. and globally. The 2009 SANDIA Labs Report[1] and the 2008 National Supervisory Control and Data Acquisition (SCADA) Testbed actions reports documented security concerns, both raising the potential impact of cyber-borne virus attacks on electrical power systems. Recommendations in this report reflect a comprehensive understanding of IT security teams mission requirements and address the growing needs of ensuring the safety, security, and resilience of Industrial Control Systems (ICS) and SCADA systems.

SECTION 2) U.S. DEPARTMENT OF DEFENSE (DOD) AND INTELLIGENCE COMMUNITY (IC) POLICIES AND BEST PRACTICES

The Body of Knowledge Annexes to this report includes a comprehensive list of references cited here. For example, the Committee on National Security Systems (CNSS) Policy on Wireless Systems directs departments and agencies to safeguard national security systems when using wireless technologies. This all-inclusive document delivers specific wireless guidance to department and agency employees, contractors, and visitors regarding reviews, management controls, operational controls, and technical controls. The CNSS wireless policy includes 14 references (Annex A) and 17 Federal, DOD, and IC guidelines conveying best practices (Annex B).

Across the DOD and the IC, the 2002 Federal Information Security Management Act (FISMA) provides Federal standards, policies, and law, and requires the U.S. National Institutes of Standards and Technology (NIST) establish technical specifications for the implementation of security control mechanisms across all Federal networks (Annex A). The NIST requires organizations apply security and privacy controls to wireless technologies as a countermeasure to the use of pervasive tracking technologies. The latest release of NIST 800-53, Security and Privacy Controls for the Federal Information Systems and Organizations states all wireless devices and networks are subject to monitoring and privacy rules. Other NIST publications applicable to the lab environment include NIST 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations and the NIST family of publications listed in CNSS Policy on Wireless Systems, Annex B. Related to FISMA implementation and the NIST is the **Risk Management Framework (RMF)** in practice across DOD and the IC. RMF (Annex B) helps organizations manage information security risks, including wireless, throughout the system development life cycle and should be adapted to IT security activities.

Internet of Things (IOT) and ICS assurance is essential given the unique cyber risks wireless communications can introduce, such as the interception and monitoring of data, wireless frame spoofing, and denial-of-service attacks. ICS assurance best practices include using device authentication and data encryption methods that align with Institute of Electrical and Electronics Engineers (IEEE) 802.11 and the IEEE 802.15.4 protocol standards. These are becoming the standards for deploying reliable and secure wireless networks for IACS applications.

[1] SAND2009-1673 - Stamp, Laviolette, Phillips, & Richardson, 2009.

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
mcoleman@vtscyber.com
ccopeland@vtscyber.com
703.498.2150 703.498.2149

Today with the IoT and the coming "second (automation-based) industrial revolution," hackers and adversaries have the opportunity to take control of insecure devices. This control enables them to conduct disruptive or destructive attacks on critical infrastructure, manufacturing technologies, and in extreme cases, the trusted supply chains for critical components used in support of national security and defense. Accordingly, this causes security risks to information within the IEEE 802.15.4 spectrum standards. While cyberattacks pose only nominal risk to short range mesh networking devices, other non-terrestrial based wireless communications mediums, such as WiFi, pose significant risk when compared to IEEE 802.15.4 standards-based technologies. Examples of the four industrial wireless communication technologies and categories of sensor networking devices; sensor and local area networking; cellular local area and backhaul communication; and low power wide area networks (LPWAN) and satellites include the following:

- **WirelessHART** is an open-standard wireless technology developed by HART Communication Foundation for use in the 2.4 GHz ISM band. WirelessHART uses IEEE802.15.4 for the lower layers and provides a time-synchronized, self-organizing, and self-healing mesh architecture.
- **ISA100.11a** is an open-standard wireless networking technology developed using Industry Standard Architecture (ISA). It is a wireless system for industrial automation including process control and other related applications.
- **Zigbee**, supported by the Zigbee Alliance, provides higher level bands required for low powered radio system for control applications including lighting, heating, and many other applications.
- **RF4CE** (Radio Frequency for Consumer Electronics) has amalgamated with the Zigbee alliance and aims to provide low power radio controls for audiovisual applications, mainly for domestic applications such as commercial cable boxes and televisions. It is unlikely to be included in technologies used within industrial automation. However, activities should exercise due diligence to avoid potential risks when implementing this technology in spaces shared with industrial automation, such as break areas near control or monitoring stations, or audiovisual devices in use on plant floors for informational or employee entertainment purposes.
- **Bluetooth** is an open-standard wireless technology standard managed by the Bluetooth Special Interest Group. It exchanges data in short-range radio frequency communication between fixed and mobile devices.
- **MiWi** and the accompanying MiWi P2P systems designed by Microchip Technology enable low data and short distance transmission rates. These low cost networks are aimed at applications including industrial monitoring and control, home and building automation, remote control, and automated meter reading.
- **6LoWPAN** is an acronym for "IPv6 over Low power Wireless Personal Area Networks." It is a system that uses the basic IEEE 802.15.4, but uses packet data in the form of IPv6.
- **WiFi** is a low power local radio frequency based communications platform, widely used in both public and private networks for local communications capabilities. While this can be used in an industrial setting, the known vulnerabilities are many. All areas should be actively monitored and managed for threat vectors such as rogue access points and interferences through a dedicated 24/7 security operations team.
- **Private 4G/5G and Low Latency 5G** both provide a solid solution for industrial applications. However, moving into highly secured and controlled operations it is recommended that ONLY the private 5G capability be considered. Though we see industry examples of cloud-to-machine and/or cloud-to-robot applications of 5G capabilities that are very successful, due to mission requirements and security functions, publicly available and widely used cloud service providers should be avoided in the architectures.

DOD and IC policies exist for some of these technologies, including for Bluetooth (NIST 800-121). Agencies also publish their own policies governing specific uses also, for example the National Security Agency's (NSA's) "Bluetooth for Unclassified Use" policy in 2015. It is robust in its guidance for specific versions of Bluetooth capable devices, the security mechanisms for each version of Bluetooth, and general guidance on how to secure personal use devices to mitigate against potential threats and vulnerabilities.

Currently, within DOD and the IC, including the NSA, there is a primarily "zero tolerance" policy for all personally owned wireless devices in secure spaces, regardless of type of technology in use. Additionally, with the exception of Bluetooth and WiFi, there is rarely, if ever, guidance or policy addressing the specifics of technologies such as Zigbee, Miwi, and other 802.15.4 based wireless communications protocols. The IC has been directly involved in the study of the security requirements, protocols and policies in anticipation of the use of these technologies. The NSA in particular has

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
mcoleman@vtscyber.com
ccopeland@vtscyber.com
703.498.2150 703.498.2149

performed much research into the encryption requirements, data use types, and proper implementation of many of these technologies, with special consideration given to both open source encryption mechanisms, such as WirelessHART and ISA 100.11a, and more proprietary capabilities such as MiWi. With the stand-up of the new NSA Cybersecurity Directorate, the Director of NSA announced this Directorate focus on the resilience of key critical infrastructure sectors, to include research, testing, and policy development.

SECTION 3) CASE STUDIES

Throughout this section, case studies on aspects discussed are further explained at the hyperlinks in Annex C which includes additional illustrative case studies. According to commercial industry customer research, the industrial community's highest current concern is the need to test and certify IACS' cybersecurity. ICS manufacturers are starting to (or may soon be required to) include security requirements in the design phase of ICS components and applications. However, independent evaluations currently do not exist and are needed to effectively guarantee those devices are secure and interoperable when including new security features and capabilities. **Penetration testing and auditing** in controlled laboratories shows that developers can identify basic security bugs in devices and applications by including security development best practices during the development cycle. Currently, the required steps to mitigate cyber risks falls to the engineers responsible for each individual installation instance. And engineers and designers of these technologies stay focused on the near-term development of assurance solutions and practices that industry can adopt and integrate. Below, includes industry standard security mechanisms inherent to each of the non-Wi-Fi based, close-range technologies in use by large commercial industry players today:

WirelessHART uses a group of robust security measures to protect the network and secure data. Features include:

- Robust, multi-tiered, always-on security
- Industry standard 128-bit Advanced Encryption Standard (A)ES encryption
- Unique encryption key for each message
- Data integrity and device authentication
- Rotated encryption keys used to join the authentication failures network – automatic or on-demand
- Channel hopping for security protection and co-existence
- Indication of failed access attempts, perhaps by a rogue device
- Reports message integrity
- Safe from W-Fi type internet attacks
- Multiple levels of security keys for access

Security for WirelessHART is built in and cannot be disabled. It is implemented with end-to-end sessions using industry standard AES-128-bit encryption approved by NSA for top secret information. These sessions ensure that messages are enciphered so only the destination device can decipher and use the payload created by a source device.

MiWi considers the physical aspect of wireless communication, and therefore addresses the content of the information exchange over-the-air (OTA). This OTA content is equally easy to access for all parties, either intended or unintended listeners, and securing the packets is essential to some applications. Among all the popular security engines in the public domain, the candidates which have no internet protocol (IP) issues include:

- Data Encryption Standard (DES)/Triple DES (TDES)
- Blowfish/Twofish
- Serpent
- AES
- Tiny Encryption Algorithm (TEA/XTEA/XXTEA) Family

Low-cost implementation ensures the security module can be implemented on a low-cost microcontroller (MCU) with limited system resources and computation speed. DES/TDES is known to be complex and require more system resources relative to their security strength. Blowfish/Twofish, Serpent, and AES provide more secured algorithms, and the implementation is simpler than DES families. However, the system resources required for these ciphers are higher than expected for an embedded system. AES is usually the preferred choice of security for the industrial, scientific, and medical (ISM) band protocols related to the IEEE 802.15.4 standard. Typical implementation of these encryption engines requires at least a 4 Kbyte programming space. However, the standard implementation of a TEA family requires approximately 200 bytes of programming space, and the speed of execution is faster.[2] Considering the system resources for an embedded system, the security engines of a TEA family meet most IACS cybersecurity requirements.

[2] AN1371- Microchip MiWi™ Pro Wireless Networking Protocol. Microchip Technology Inc. Yifeng Yang, 2011.

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
mcoleman@vtscyber.com
ccopeland@vtscyber.com
703.498.2150 703.498.2149

One of the greatest advantages of XTEA, as opposed to others on the list, including those within the TEA encryption family, is that the system resources required to encrypt or decrypt the information are very limited. The volatile memory requirement for XTEA is extremely low compared to other security engines with similar strength. Therefore, the XTEA is best suited to be used in embedded systems with few resources. Additionally, XTEA's required resources and the complexity of the algorithm can be fine-tuned by applying different round times to the algorithm. Fewer rounds can perform the algorithm faster, and the complexity decreases linearly with the rounds. However, it is easier to break the algorithm with fewer rounds. For wireless applications that Microchip Wireless Media Controller Interface (MiMAC) serves, the required security level and response time significantly varies. The capability of easily adjusting the security level and system resource requirement in XTEA is valuable for working with a wide range of applications.

The **smart home** device industry is only getting bigger. According to Statista (2021) industry outlook:

- Revenue in the Smart Home market is projected to reach US$28,864m in 2021.
- Revenue is expected to show an annual growth rate (CAGR 2021-2025) of 12.8%, resulting in a projected market volume of US$46,767m by 2025.
- Household penetration will be 40.0% in 2021 and is expected to hit 57.2% by 2025.
- The average revenue per installed Smart Home currently is expected to amount to US$552.78.
- A global comparison reveals that most revenue is generated in the United States (US$28,864m in 2021).

By 2025, this market projection has over 50% household penetration. Over half of the homes will have these smart devices up and running inside. These devices have an inherent risk involved. They are internet capable. Like any internet device certainly there are steps any consumer can to take to harden them. Buts these steps fall short of one thing: Better devices.

"The exact rate of security breaches is unknown. Manufacturers don't disseminate this information and it doesn't fall under the purview of any one regulatory body." Ferron (2020)

No regulatory body means no standardization. Beyond that, improvements to a device are entirely left the manufacturers discretion. Updates only upon a vulnerability exploited.

In their current state, irresponsibly implementing these technologies around your home can put your personal privacy and safety at risk. Kellermann (2019)

Another approach is needed.

The desire for smart homes and devices is not likely to subside, ever. As well, cyber attackers and cyber attacks are not likely to fade. The adoption of the Risk Management Framework (RMF) directly into the development of these devices. The creation of an industry wide standard. A standard which is not only proven, but also evolves as the technological landscape changes. Consumers will always desire creature comforts and easing of household tasks. These devices, however, should not put the consumer at undue risk of cyber-attacks.

ISA100.11a, like WirelessHART, defines a set of security keys used to ensure secure communication. Symmetric cryptography relies on both communication end points using the same key when communicating securely. Attackers that do not share the keys cannot modify messages without being detected and cannot decrypt the encrypted payload information. Common to both standards is that a new device is provisioned with a join key before it attempts to join a network. The join key is used to authenticate the device for a specific network. Once the device has successfully joined the network, the security manager will provide it with keys for further communication. The use of the join key is optional in ISA100.11a. A global key, a well-known key with no security guarantees, may also be used in the join process for devices not supporting symmetric keys. ISA100.11a allows for optionally encrypting messages. ISA100.11a Over the Air Provisioning (OTAP), in combination with asymmetric keys is useful for scaling up networks. WirelessHART does not allow security to be optional which prevents mistakes that can compromise the system.

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
mcoleman@vtscyber.com
ccopeland@vtscyber.com
703.498.2150 703.498.2149

Architecture Considerations
In consideration of the two different wireless local area network (WLAN) architecture types used in IACS settings, security is of paramount concern. An **autonomous architecture** type uses standalone wireless access points to implement all WLAN functions. Each autonomous access point is individually configured and managed. An autonomous architecture is typically used only for small-scale deployments or standalone wireless applications. It has a lower initial hardware cost, simplified design and deployment, and offers more granular control of quality of service to help prioritize IACS application traffic on the network. A **unified architecture** (UA), used for large-scale, plantwide deployments, requires a wide range of clients and applications. Offering more robust foundational services, this architecture allows for the inclusion of intrusion prevention and wireless guest access, provides the foundation for enabling plantwide mobility, and can be managed centrally or even remotely. This architecture solution splits functionality between light weight access points (LWAP) and wireless LAN controllers (WLC). It has "zero touch" deployment and replacement of access points, requires less effort for updating configuration and firmware, and provides centralized control and visibility.

SECTION 4) SOLUTIONS

It is common to assume that protocol standards establish basic levels of security requirements and policies. However, much of that is incumbent upon the various technology developers and even more so, on the implementors of each of the technologies in use. Through in-depth research and analysis of the current DoD, IC, and industry landscape, it is our recommendation that IT security leadership ensure that the following mechanisms are in place when moving forward in their implementation of any wireless communication technologies:

1. **Ensure a robust executive level policy is in place for the entire organization.** This policy should include coverage of both authorized and unauthorized uses of non-terrestrial wireless communications capabilities. It should also specify those specific technologies that are and are not authorized within specific areas of use. Consider establishing an executive Wireless Network Policy Group and a framework for biannual online compliance audits, incorporated in current security, safety, and resilience regimes.
2. **Publish a Wireless Risk Framework.** Following a template similar to the RMF, create a Wireless Risk Framework so that all stakeholders (i.e. engineers, security personnel, operators, vendors and mission owners) are aware of security requirements, steps to mitigate potential threats, and when and how those steps are applicable.
3. **Map all guidance to a Wireless Risk Framework.** Including guidance from federal agencies such as NIST and NSA, as well as independent/private organizations such as IEEE and ISA.
4. **Ensure the Wireless Risk Framework is implemented, trained to, and complied with.** These bodies are specifically designated with the express purpose to ensure that standards are upheld, implemented properly, and securely addressed across any communications architecture, and to include periodic updates and refresher training.
5. **When implementing industrial automation communications technologies, ensure the technology is secure, does not inhibit secure use by operators, and is conducive to the use environment.**
6. **Use the following recommended technologies in industrial control situations for government use: WirelessHART, ISA100.11a, and MiWi (MiMAC – XTEA only).**
7. **Do not use the following technologies which are not recommended in most industrial settings: Wi-Fi, RF4CE, and Zigbee.**

SECTION 5) CONCLUSION

Virescit Tactical Systems specializes in in the creation, implementation, governance, and training for customer specific risk management and mitigation frameworks and policies. VTS staff has a vast amount of in-house experience with using security tools to secure an environment and creating strategies to protect against new and developing threats. With VTS a full Wireless Risk Framework can be tailored and executed to an organization's specific needs, as well as monitored and updated post-implementation. The Virtus 3 solution creates a security framework, a plan for compliance, and monitoring of threats allowing your organization to be assured that the proper security controls to protect your devices connected to the internet are being followed.

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
mcoleman@vtscyber.com
ccopeland@vtscyber.com
703.498.2150 703.498.2149

BODY OF KNOWLEDGE [3]

ANNEX A
INDUSTRY GUIDANCE

1. *"Threat Intelligence Report Says IoT Attacks Doubled Within a Year, Predicts an Upward Trend." CPO Magazine, 30 Oct. 2020, www.cpomagazine.com/cyber-security/threat-intelligence-report-says-iot-attacks-doubled-within-a-yearpredicts-an-upward-trend/*
2. *Committee on National Security Systems (CNSS) Policy No. 22. National Information Assurance Risk Management Policy for National Security Systems. 2009. Available at: http://gravicom.us/downloads/docs/CNSSP_22.pdf*
3. *NIST Special Publication **800-121 Revision 2**: Guide to Bluetooth Security. 2017. [online] Nvlpubs.nist.gov. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf*
4. *NIST Special Publication **800-153**: Guidelines for Securing Wireless Local Area Networks (WLANs). 2012. [online] Nvlpubs.nist.gov. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf*
5. *NIST Special Publication **800-160**: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. 2016. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf*
6. *NIST Special Publication **800-171**: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. 2015. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf*
7. *NIST Special Publication **800-64 Revision 2**: Security Considerations in the System Development Life Cycle. 2008. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf*
8. *NIST Special Publication **800-97**: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. 2017. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf*
9. *NIST. A Sensor Model for Enhancement of Manufacturing Equipment Data Interoperability. 2012. Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=911959*
10. *Special Publication **800-53 Revision 4**: Security and Privacy Controls for Federal Information Systems and Organizations. 2013. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*

ANNEX B
POLICY AND INDUSTRY BEST PRACTICES

1. *Cichonski, J., Marron, J. and Hastings, B. SECURITY FOR IOT SENSOR NETWORKS: Building Management Systems Case Study. 2019. Available at: https://www.nccoe.nist.gov/sites/default/files/library/projectdescriptions/iot-sniot-sensornetwork-project-description-draft.pdf*
2. *CISCO. Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design & Implementation Guide. 2014. Literature.rockwellautomation.com. Available at: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_en-p.pdf*
3. *Committee on National Security Systems (CNSS). Policy on the Use of Commercial Soluti9ons to Protect National Security Systems. CNSPP No.7. 2015. Available at: http://www.cnss.gov/CNSS/openDoc.cfm?gSRXQTuHw11SySfcKDNqzw==*
4. *Defense Information Systems Agency. Wireless Security Technical Implementation Guide Version 6, Release 1. 2009.*
5. *Department of Defense (DOD). Mobile Device Security Best Practices. Available at: https://dpcld.defense.gov/Portals/49/Documents/Media/BestPractices%20(PDF).pdf*
6. *Department of Energy (DOE). Quadrennial Technology Review 2015. Chapter 6: Innovating Clean Energy Technologies in Advanced Manufacturing Technology Assessments. 2015. Available at: https://www.energy.gov/quadrennial-technology-review-0*
7. *Department of Homeland Security. Study on Mobile Device Security. 2017. Available at: https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf*
8. *NIST Special Publication **800-124**: Guidelines on Cell Phone and PDA Security. 2008. Available at: https://csrc.nist.gov/csrc/media/publications/sp/800-124/rev-1/final/documents/draft_sp800124-rev1.pdf*

[3] Body of Knowledge (BOK), as used in this report, is defined as the depth and breadth of knowledge, skills, and outlooks applicable to practice cybersecurity and activities. Within BOK:
- Knowledge consists of comprehending theories, principles, and fundamentals
- Industry Guidance
- Government Agency Policy
- DoD and IC policies best practices
- Case Studies

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
mcoleman@vtscyber.com
ccopeland@vtscyber.com
703.498.2150 703.498.2149

9. *NIST Special Publication **800-37 Revision 1**: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. 2009. Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf*
10. *NIST Special Publication **800-39, DRAFT**: Managing Risk from Information Systems: An Organizational Perspective. 2008. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf*
11. *NIST Special Publication **800-48, Revision 1**: Guide to Security Legacy IEEE 802.11 Wireless Networks. 2008. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-48r1.pdf*
12. *NIST. Cybersecurity for Smart Manufacturing Systems. 2018. Available at: https://www.nist.gov/programs-projects/cybersecurity-smart-manufacturing-systems*
13. *NIST. Smart Manufacturing Systems Readiness Level (SMSRL) Tool. 2019. Available at: https://www.nist.gov/services-resources/software/smart-manufacturing-systems-readinesslevel-smsrltool*

ANNEX C
CASE STUDIES

1. *Gallagher, S. The Navy's newest warship is powered by Linux. 2013. Available at: https://arstechnica.com/information-technology/2013/10/the-navys-newest-warship-ispowered-by-linux/*
2. *SANS Institute: Reading Room - Industrial Control Systems / SCADA. 2016. Available at: https://www.sans.org/reading-room/whitepapers/ICS/constructing-measurable-tabletopexercise-scadaenvironment-36817*
3. *SANS Institute: Reading Room - Mobile Security: BYOD Security Implementation for Small Organizations. 2017. Available at: https://www.sans.org/readingroom/whitepapers/mobile/byod-security-implementation-small-organizations-38230*
4. *Verizon. Data Breach Digest. 2018. Available at: https://enterprise.verizon.com/resources/reports/2018-data-breach-digest.pdf*

ANNEX D
GOVERNMENT AGENCY POLICY

1. *Department of Defense DIRECTIVE. Use of Commercial Wireless Devices, Services, And Technologies in The Department of Defense (DOD) Global Information Grid (GIG). 2007. Available At: Https://Www.Esd.Whs.Mil/Portals/54/Documents/DD/Issuances/Dodd/810002p.Pdf*
2. *Office of The Chief Information Officer of The Department of Defense. DOD Instruction 8420.01: Commercial Wireless Local-Area Network (WLAN) Devices, Systems, And Technologies. 2017. Available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/842001_dodi_2017.pdf?v er=2017-11-03-092912-313*
3. *United States Agency International Development (USAID). Wireless Standards and Guidelines. A Mandatory Reference for ADS Chapter 545. 2019. Available at: https://www.usaid.gov/sites/default/files/documents/1868/545mbg.pdf*

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
mcoleman@vtscyber.com
ccopeland@vtscyber.com
703.498.2150 703.498.2149