CYBERSECURITY FOR ADVANCED MANUFACTURING

a
White Paper
prepared by
National Defense Industrial Association's
Manufacturing Division
and
Cyber Division

May 5, 2014

PREFACE

DoD and industry have focused much effort on protecting technical information in business and engineering information systems. Relatively less action has been taken to improve protection of technical data in factory floor networks and control systems, which are increasingly subject to cyber threats. Cybersecurity on the factory floor merits increased DoD and industry attention.

NDIA's Manufacturing Division and Cyber Division have jointly developed this White Paper to heighten awareness of the emerging threats, vulnerabilities and consequences in the Industrial Control Systems used in manufacturing. Better practices and technical solutions are needed to protect against theft of technical data transiting or residing in manufacturing systems, alteration of the data (thereby compromising the physical parts produced), or interference with reliable and safe operation of a production line. Solutions must be cost effective, especially for smaller manufacturers in defense supply chains. This White Paper offers several recommendations for enhancing protection of technical data in factory floor networks and control systems.

NDIA wishes to acknowledge the authors, contributors and reviewers of this report (Appendix 1), with special thanks to the many government and industry subject matter experts (Appendix 2) who graciously consented to data collection interviews.

Overview

This paper reports the results of NDIA's study of the need to protect unclassified controlled technical information in manufacturing. It addresses the unique needs of cybersecurity for manufacturing systems and networks in general, and for the Defense Industrial Base (DIB) in particular. It was prepared by a Joint Working Group of the NDIA Cyber and Manufacturing Divisions (Appendix 1).

The objectives of the paper are to raise awareness of needs, identify known solutions and best practices, point out gaps and recommend courses of action to better manage cybersecurity risks in defense manufacturing networks. The study is based on information gleaned from a literature review and a highly informative series of interviews with senior stakeholders in government, industry and academia (Appendix 2). Key findings from the study include:

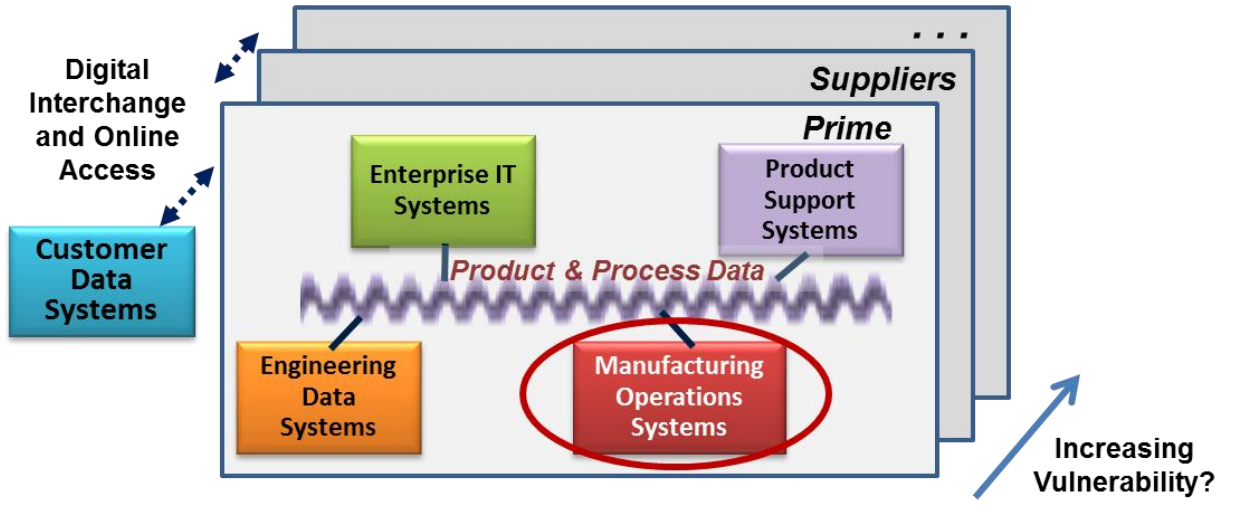
- The threat is real and manufacturing companies are targets
- Factory floor systems are a weak link in safeguarding technical information
- Small Business manufacturers are not well equipped to manage the risks

The last section of the paper presents recommendations for DoD to work with industry to heighten awareness and improve cybersecurity in Defense supply chain manufacturing systems.

Protecting the Digital Thread

Defense contractors throughout DoD's supply chain have been targeted by cyber criminals attempting to steal unclassified technical data. Concerned about potential damage to national security, in November 2013 DoD issued a new contract clause,[1] with mandatory flow-down to subcontractors, requiring defense contractors to incorporate established information security standards on their unclassified networks and to report cyber-intrusion incidents that result in the loss of unclassified controlled technical information. Implementation of this requirement will require DoD and industry to work together to manage risks at every level of the enterprise, including the factory floor.

Figure 1 – Protecting the



Digital Thread

[1] **Federal Register** /Vol. 78, No. 222 /Monday, November 18, 2013 /Rules and Regulations **69281** (http://www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27313.pdf)

The factory floor is a growing area of concern for cybersecurity. In much of the Defense Industrial Base (DIB) manufacturing is digitally driven. The era of skilled machinists operating from paper engineering drawings has given way to networks of computers, automated machines, ubiquitous sensors, and technicians whose job is to convert digital data into physical parts and assemblies. Design, manufacturing and product support operations are driven by a "digital thread" of technical data -- product and process information -- that can be shared throughout the supply chain and must be protected. Much attention has been given to protecting technical information in information technology (IT) systems and networks. But protecting the *operational systems* of a manufacturing enterprise presents a new and different set of challenges. Not only must the technical data be protected from theft, it must also be protected from alteration that could impair the proper functioning of parts produced or affect the safety and availability of the production system. These concerns are especially challenging for small and mid-size manufacturers.

The Threat is Real, and Manufacturing Companies are Targets

Cyber threats to manufacturing enterprises may be motivated by espionage, financial gain or other reasons to compromise data Confidentiality, Integrity or Availability – the C-I-A concerns that are the focus of IT cybersecurity[2]. For the advanced manufacturing enterprise, these concerns are translated as:

1. Theft of technical data, including critical national security information and valuable commercial intellectual property. *This is a Confidentiality concern.*
2. Alteration of data, thereby altering processes and products. *This is an Integrity concern.*
3. Impairment or denial of process control, thereby damaging or shutting down operations. *This is an Availability concern.*

These concerns exist from the point of creation of the technical data, through its access at any point in the supply chain, to its use to control physical manufacturing processes throughout the product life cycle. There is ample cause for concern. Symantec reports that manufacturing was the most targeted sector in 2012, accounting for 24% of all targeted attacks.[3] State-sponsored data breaches became the second most common variety of data breaches in 2012, following only organized crime, according to a study by Verizon.[4] McAfee's 2012 Threat Predictions identifies industrial networks as the leading cybersecurity vulnerability, and states, *"Attackers tend to go after systems that can be successfully compromised, and ICS [industrial control systems] have shown themselves to be a target-rich environment."*[5] Cyber spies, cyber criminals, cyber terrorists, disgruntled insiders and hacktivists can attack in very sophisticated ways. For example, the Washington Post (May 28, 2013) reported that a cyber espionage Advanced Persistent Threat (APT) exfiltrated technical design data on over two dozen US defense systems. Mandiant[6] provided details on a class of sophisticated APTs that is traceable to China, and that took most victim companies months to discover and additional months to mitigate – a long window during which sensitive intellectual property was being compromised. Stuxnet,[7] the worm that attacked the Iranian uranium refinement capabilities, was a sophisticated attack targeted to specific

[2] ISA (2013), "NIST Cybersecurity Framework ISA99 Response to Request for Information," April 5, 2013, Research Triangle Park, NC: ISA, p3. (http://csrc.nist.gov/cyberframework/rfi_comments/040513_international_society_automation.pdf)
[3] Symantec Internet Security Threat Report - 2013, p15 (www.symantec.com)
[4] Verizon 2013 Data Breach Investigations Report, p21 (http://www.verizonenterprise.com/DBIR/2013/)
[5] McAfee 2012 Threat Predictions, p3 (http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf)
[6] Mandiant Intelligence Center APT1 report (http://intelreport.mandiant.com/)
[7] Symantec W.32 Stuxnet Dossier (http://www.symantec.com)

machine controllers similar to those widely used in manufacturing operations. Hackers attacked Lubrizol, an Ohio-based chemicals company, through ICS to steal intellectual property causing substantial financial damage.[8] Threats like these are hard to detect and containment/restoration can take months. Fortunately, according to Verizon, such sophisticated attacks are not yet commonplace. Over 70% of the attacks examined in 2012 were of low or moderate sophistication, but this should not be cause for complacency. As Verizon[9] puts it, "Would you fire a guided missile at an unlocked screen door?"

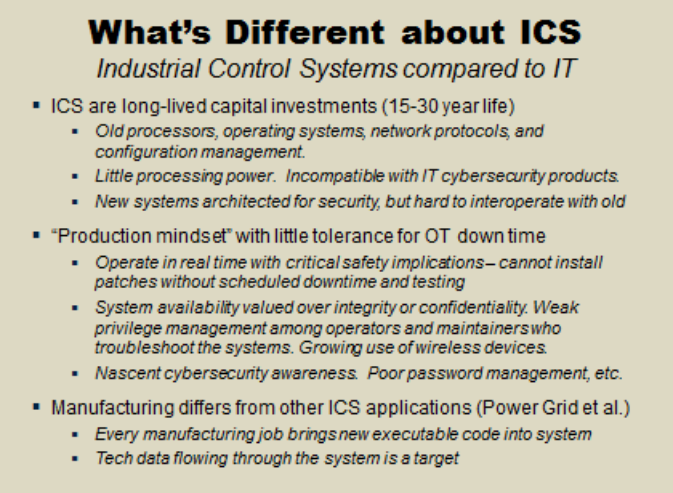
Manufacturing Needs and Priorities Differ from Business IT Systems

Much of the current attention to cybersecurity is focused on information technology (IT) systems that, in large organizations, are usually under the purview of a Chief Information Officer (CIO) or Chief Information Security Officer (CISO). CIOs and CISOs in large defense firms are implementing strong cyber risk management standards, technologies and practices. Their participation in DoD's DIB Cyber Security/ Information Assurance (CS/IA) program and the Defense Security Information Exchange (DSIE), an NDIA cyber threat sharing committee, has been a model for industry-government and industry-industry collaboration on complex issues. Interviews conducted for this study revealed that large companies:

- Are confident in their risk management posture but are concerned about suppliers, especially small businesses, who lack the resources and knowledge to identify and mitigate cyber risks. Large companies are concerned that supplier vulnerabilities could become their vulnerabilities, and are willing to work with suppliers on improvements.
- Have not yet seen an upsurge in the threat to factory systems, but acknowledge the growing interconnections between factory systems and other systems, and the existence of targeted attack examples. They do not want manufacturing systems to be the weak link in the enterprise.
- View increased mandatory cyber protection requirements with concern unless they are accompanied by funding for implementation. They advocate use of voluntary commercial standards and practices where possible, and advocate a process of cost/risk tradeoffs to arrive at affordable solutions for cybersecurity in the DIB.

[8] "High-impact Threats to Critical Infrastructure," *Proceedings of the Policy Studies Organization 22* (December 2012): 92 (http://www.ipsonet.org/proceedings/wp-content/uploads/2013/08/Proceedings-22-reduced.pdf)
[9] Verizon, Op. Cit., p 49 (http://www.verizonenterprise.com/DBIR/2013/)

In assessing how to extend the CIO/CISO IT thinking into applications in manufacturing systems, it is important to recognize the similarities and differences between the manufacturing operational technology (OT) culture and the information technology (IT) environment and culture. Factory floor technology includes networks, servers and end point computers, but it also includes cyber-physical systems where networked machines, sensors and software combine to produce physical changes in materials, parts and environments. The Industrial Control Systems (ICS) that control these processes typically run specially designed operating systems and communications protocols, handle real-time processing and synchronization needs, have a lifetime on the order of 15-20 years, are rarely rebooted or stopped to install patches, depend on networked sensor feedback, and can have catastrophic physical safety consequences if they are compromised. ICS outages may need to be scheduled weeks in advance. While cybersecurity is deeply ingrained in the IT culture, the Operations Technology (OT) culture is focused first and foremost on safety and availability of factory systems for production output. Technicians, including those from the original manufacturer, often have administrator privileges, and use them creatively to keep the machines running. In essence, digits (executable files from global sources) go into the factory and parts come out, often with limited ability to screen the files or the resulting products for integrity.



In the past, most ICS networks were autonomous and built upon proprietary vendor technology. ICS solutions were geared towards speed, functionality, reliability and safety. Cybersecurity features were not a high priority when there was an air gap between ICS networks and other networks in the enterprise. Today, however, competitive pressures are driving the integration and analysis of "big data" collected from business information systems, engineering information systems and manufacturing systems across the supply chain. Organizations need to respond quickly to market changes and they need to manage operations and maintenance with fewer people. Executives need timely and accurate information. Production control systems – ICS – must feed this information to the decision makers as soon as possible.[10] Several interviews conducted during this study indicated a distinct trend toward integration of IT and OT systems. Manufacturing enterprises handle a wide range of sensitive data through their highly connected relationships with customers, suppliers and equipment vendors. In the future, enhancing ICS cybersecurity must be addressed as an integral part of enterprise security.

[10] Honeywell White Paper, Cybersecurity in Manufacturing and Production, WP 686, August, 2011, Http://www.honeywell.com/ps

The community of ICS vendors, users and standards organizations has made significant strides in enhancing ICS cybersecurity. Both the ISA99 series of international standards for Industrial Automation and Control Systems, and NIST's Guide to ICS Security (SP 800-82) recognize these unique needs (see Appendix 3) and identify best practices to mitigate risks. These standards and guides also define a comprehensive set of good practices that the providers and owners/operators of ICS technologies use in critical infrastructure systems (e.g. nuclear industry, power grid, chemical industry). Implementation in manufacturing is, at present, spotty.

Additive Manufacturing

An interesting microcosm of what happens on the cyberphysical factory floor is evident in Additive Manufacturing, also known as 3-D printing. This process can make a three-dimensional solid object of virtually any shape from a digital model, and the palette of materials is growing from plastics to metals and composites. It is rapidly evolving as a production method for functional parts, such as cooling ducts in the F-35 and parts for turbine engines. For the DoD, its ability to produce small quantities efficiently (lot size of one) makes it particularly attractive. Information about materials, finish, and other physical attributes are all contained in the digital production (print) file – which makes this file a critical piece of intellectual property to protect for both competitive and national security reasons. Recent experiments by Virginia Tech Applied Research Corporation have shown typical additive manufacturing operations will be a soft target for hackers wishing to alter the properties or features of the manufactured item in hard-to-detect ways. While additive manufacturing is inherently no more vulnerable than other manufacturing methods, the opportunity exists to build more security into these emerging systems now.

ICS component vendors and integrators build their latest products with cybersecurity in mind. The installation of new ICS networks in manufacturing plants is architected to protect vulnerable network interfaces. Users are advised to implement the best practices documented in ICS standards, guides and vendor manuals. Unfortunately, the long operational life of older ICS equipment and the challenges of integrating new equipment with older systems inhibit full implementation of the known cybersecurity solutions. For the human element of the system, changing the factory floor culture to embrace good cybersecurity hygiene is a slow process. And from a technology standpoint, manufacturing applications have needs that differ from the other ICS applications that have been the primary drivers of solutions. In continuous operations such as the power grid or the transportation system, the priority is to protect the safe operation of the ICS itself. In manufacturing, the additional priority is to protect the data residing in or transiting through the ICS from theft or alteration. DoD's emphasis on technical data protection will require continued development of technologies, standards and practices for data protection on the factory floor.

Small and Mid-Size Firms Face Large-Size Challenges

Defense prime integrators are concerned about their suppliers' ability to manage cybersecurity risks. Technical data packages, process flows and other critical information move up and down the supply chain in business transactions and in engineering collaborations. While most large corporations have made significant improvements in their business information technology network protections, research for this report found only an emerging awareness of the threats to the manufacturing information networks. Additionally, the lower tier DIB contractors struggle to secure their business networks and most have not initiated protection of their manufacturing networks.

McAfee's 2012 Threat Predictions[11] identifies industrial networks as the leading cybersecurity vulnerability, and states, *"Attackers tend to go after systems that can be successfully compromised, and ICS systems have shown themselves to be a target-rich environment."* Many smaller suppliers do not

[11] McAfee, Op. Cit., p3 (http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf)

have the resources, expertise or financial incentives to identify vulnerabilities and mitigate risks. Their ICS networks are typically vulnerable to backdoors, default passwords, discoverable IP addresses, connection by portable devices and connection from outside networks. Small manufacturers often believe that they are not likely to be targets of cyber attacks, and that perimeter defenses such as firewalls and virus protection will keep them safe -- a false hope in light of recent data.

Verizon's 2013 Data Breach Investigation Report (DBIR) found that manufacturing networks are more likely to be targeted for purposes of espionage than for financial gain, and operations with fewer than 1,000 employees are more often targeted than the large corporations.[12] While the Verizon sampling is not large enough to make sweeping recommendations, the data highlight the particular threat to the multi-tiered defense industrial base that contains sensitive defense system design and production information.

This concern underlies the DoD mandate to flow down to suppliers mandatory contract requirements to protect unclassified controlled technical data. NDIA's member companies want to work with DoD on implementing this mandate in a way that does not impose unrecoverable costs or introduce potential liabilities that deter suppliers from entering or remaining in the DoD market. Significant advances can be made without great expense. A recent report from the Penn State Applied Research Laboratory[13] notes that "[m]itigations against most attacks are neither expensive nor difficult. It is estimated that four mitigation techniques can prevent at least 85% of attacks."

Smaller companies, for their part, view ISA99 standards and the NIST SP 800-82 guidelines for ICS security as complex and hard to implement. Many small manufacturers have no full time cybersecurity staff. There are no turnkey solutions for protection, and available information on pertinent threats is limited or classified. The forums available to large companies for information exchange (e.g. the DIB CS/IA program) are often beyond their reach.[14] They cannot afford to deal with differing cybersecurity requirements from different customers, and therefore seek standard practices among their aerospace and defense prime integrators. Once such practices are defined, small companies will need training and implementation assistance. Aerospace and defense integrators may work through existing business collaboration forums, such as Exostar,[15] to help selected suppliers improve cybersecurity risk management. Established government programs, such as NIST's nationwide network of Manufacturing Extension Partnership (MEP) centers,[16] offer a potentially broader channel for delivery of training and assistance to small manufacturers.

A mechanism is needed to help DIB stakeholders -- DoD, defense prime integrators, and suppliers -- collaboratively define needs, adopt known solutions and best practices, and develop new solutions to fill gaps. This mechanism must meet the business needs of the manufacturing sector. The NIST-led Cybersecurity Framework initiative offers an excellent starting point for developing such a mechanism in the DIB critical infrastructure sector.

---

[12] Verizon 2013, Op. Cit. p. 14 (http://www.verizonenterprise.com/DBIR/2013/)

[13] B. Toth, C. Severn and J.Hoerr, "Understanding Security," Technical Report No. TR-13-003, 29 August 2013, The Applied Research Laboratory, The Pennsylvania State University, State College, PA.

[14] Of the entire supplier base to DoD only 2,650 companies have been identified as eligible participants, with less than 100 actively participating in such programs.

[15] www.exostar.com

[16] http://www.nist.gov/mep/

The Cybersecurity Framework for Critical Infrastructure Protection

The President's February 2013 Executive Order (EO 13636), "Improving Critical Infrastructure Cybersecurity", called for DHS-led revision of the National Infrastructure Protection Plan to enhance cybersecurity protection in 16 critical infrastructure sectors. The EO required NIST to lead development of a voluntary, technology-neutral framework to provide a common language and mechanism for organizations to use in managing cybersecurity risk. NIST's February 2014 Cybersecurity Framework for Critical Infrastructure Protection Version 1.0[17] defines the concepts and core standards and practices that apply to all critical infrastructure sectors. It is intended to be a point of departure for sector-specific organizations to build on and extend to meet sector business needs. The risk management concepts in the Framework are general enough to apply to manufacturing cybersecurity, and are supported by a Framework Core, with categories and informative references (cross-cutting standards and guides) for risk management in five key cybersecurity functions -- Identify, Protect, Detect, Respond and Recover. As Figure 1 illustrates, the Framework identifies standards and best practices relevant to each subcategory. It provides a tier-based model and target profile concepts firms can use to tailor implementation to an appropriate level of cyber risk management for their business needs.

Figure 1. Excerpt from NIST Cybersecurity Framework Version 1.0

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

During development of the Framework, NDIA comments emphasized that industry values the risk-based principles and the voluntary implementation approach the Framework provides. We believe the same risk-based principles and voluntary framework can be used as a starting point to fill gaps in cybersecurity

[17] NIST Cybersecurity Framework (www.nist.gov/cyberframework/)

for manufacturing systems. Adopting the vocabulary and principles of the Framework will facilitate efforts by companies that support the DIB to integrate and implement concepts from several areas of DoD policy that affect factory floor operations. These include cybersecurity policies, program protection policies, trusted component policies, and DFAR regulations for safeguarding unclassified controlled technical information.

An Integrated Approach to Cybersecurity for Defense Manufacturing

NDIA believes improving cybersecurity risk management in manufacturing systems requires effort at the intersection of three complementary DoD policy areas: Procurement Policy (the DFAR requirement for protecting unclassified controlled technical information); Systems Acquisition Policy (DODI 5200.39 requirements for Program Protection Plans and DODI 5200.44 requirements for Trusted Components); and Information Assurance policy (the DODI 8500.2 cybersecurity requirements).[18] We believe the new Framework offers an opportunity to build on common, commercial principles, standards and practices as DoD and DIB companies work together at the intersection of these policies to strengthen risk management in manufacturing systems.

The DFAR requirement and the Framework have already been discussed. The Program Protection Plan (PPP) required by DODI 5200.39 for major acquisition programs typically includes an Information Assurance strategy that complies with DoDI 8500.2. The PPP is a "living" document intended to help programs ensure that they adequately protect critical program information over the program's lifecycle. The DODI 5200.44 policy on Trusted Systems and Networks requires risk management for trusted components throughout the lifecycle. Although factory system vulnerabilities are an area of risk implicitly covered by these policies, there is no specific guidance on cybersecurity risk management for manufacturing in the policies. The connections must be made in company plans and program plans. For example, production of trustworthy components could be compromised by cyber penetration that alters the digital files driving manufacturing, thereby altering the functionality of the manufactured components.

Developing the guidance for cybersecurity in manufacturing systems, identifying the relevant standards and best practices, and assisting supply chain partners with voluntary implementation will require collaborative DoD and industry efforts. Commonality of expectations in business interfaces across DIB supply chains is highly desirable, and can be facilitated by adopting commercial concepts, standards and practices wherever possible. Much work remains to be done to define solutions at an implementable level of detail, but NDIA believes the Framework offers a useful point of departure for such work.

NDIA Recommendations for USD(AT&L)

1. Designate a focal point to work with industry on risk-based, voluntary standards and practices to strengthen factory floor cybersecurity in defense supply chains. NDIA is willing to take an active role in addressing factory floor issues and to facilitate DoD and industry interaction to:

    - Evaluate the core standards, practices and concepts of the NIST Framework as a starting point for improving Industrial Control System (ICS) security in manufacturing applications, with DIB sector-specific extensions as needed. Use a common vocabulary and aim for compatibility with commercial solutions wherever possible, while meeting

[18] DoDI 8500.2 Information Assurance Implementation, DoDI 5200.39 Critical Program Information Protection, DODI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (DoD Issuances Website)

national security needs. Collaboration with the DHS established and DoD managed DIB Sector Critical Infrastructure Protection Program may prove fruitful for this effort.

- Create common business interface expectations among DoD, prime contractors and suppliers for cybersecurity controls in manufacturing systems

2. Conduct a series of forums with defense prime contractors and suppliers (with special emphasis on small business participation) to improve broad understanding and implementation planning for the new DFAR clause on safeguarding unclassified technical information (including factory floor implications). NDIA would be willing to organize and host such a series.

3. Update DoD guidance on the Program Protection Plan (PPP) to address critical information that resides in or transits manufacturing systems and networks. Let industry make appropriate risk/cost tradeoffs in developing PPPs for DoD review.

4. Expand the use of red teams to identify manufacturing system cybersecurity vulnerabilities, and identify specific capabilities that need strengthening. Sponsor R&D (including S&T and SBIR programs) to develop better data protection capabilities in industrial control systems and networks used in manufacturing, with the goal of dynamic mitigation of cyber threats in high availability, safety-critical, real-time manufacturing operations.

5. Develop programs to facilitate manufacturing system cybersecurity in defense supply chains

    - Work with the NIST Manufacturing Extension Partnership network and other delivery channels to develop and deliver training to small and mid-size manufacturers and assist them in implementing cybersecurity principles, standards and practices to meet the needs of DoD and DIB trading partners.

    - Provide incentives and, where justified, investment assistance for capital investments to upgrade and strengthen ICS systems and networks. Investigate applicability of the Manufacturing Technology program and Defense Production Act Title III authorities for use in improving cybersecurity for assured domestic sources of supply.

    - Develop Defense Acquisition University training modules to familiarize the DoD acquisition workforce with cost-effective cybersecurity risk management practices and to provide training in appropriate application of contract requirements for safeguarding unclassified controlled technical information, including in manufacturing systems.

Appendix 1 – NDIA Cyber Division and Manufacturing Division Joint Working Group Members

Co-chairs:

Jennifer Bisceglie, Interos Solutions Inc. *(NDIA Cyber Division)*
Michael McGrath, Analytic Services Inc. *(NDIA Manufacturing Division)*

Study Group:

David Chesebrough, Association for Enterprise Integration
Mark Fedak, Private Consultant
James Godwin, Britewerx Inc.
Mark Gordon, National Center for Advanced Technologies
Larry John, Analytic Services Inc.
Catherine Ortiz, Defined Business Solutions, LLC
Chris Peters, The Lucrum Group

Reviewers:

William Barkman, Y-12 Babcock & Wilcox
Barry Bates, NDIA
Brench Boden, Air Force ManTech (AFRL)
Kevin Fischer, Rockwell Collins
Matthew Fleming, Homeland Security Institute
Michael Lemon, International Technegroup, Inc.
Rebecca Taylor, National Center for Manufacturing Sciences
John Vankirk, Kennametal
NDIA Manufacturing Division
NDIA Cyber Division
NDIA Systems Engineering Division
NDIA Armaments Division
NDIA Small Business Division

Appendix 2 – Subject Matter Experts Interviewed by NDIA Working Group

The working group gratefully acknowledges the not-for-attribution contributions of the following individuals and organizations:

Jon Boyens, National Institute of Standards and Technology
Elana Broitman, Office of the Secretary of Defense (MIBP)
Jaime Camelio, Virginia Tech
Eric Cosman, Dow Chemical and ISA99 Committee
Don Davidson, Office of the Secretary of Defense (CIO)
Emmanuel de la Hostria, Rockwell Automation and ISA99 Committee
Paul Didier, CISCO
Geoffrey Donatelli, Raytheon Missile Systems
Lee Holcomb, Lockheed Martin
Gregory Larsen, Institute for Defense Analyses
Daniel Massey, Department of Homeland Security
Johan Nye, Exxon Mobil and ISA99 Committee
Laura Odell, Institute for Defense Analyses
Robert Parker, VT Applied Research Corporation
Perry Pederson, The Langner Group LLC
Michael Pozmantier, Department of Homeland Security
Melinda Reed, Office of the Secretary of Defense (Systems Engineering)
Charlie Robinson, International Society of Automation (ISA)
Keith Stouffer, National Institute of Standards and Technology
Doug Thomas, Lockheed Martin
Steven Venema, Boeing
Doug Wylie, Rockwell Automation

Appendix 3 – How ICS Systems Differ from IT Systems

Source: NIST SP 800-82

Category	Information Technology System	Industrial Control System
Performance Requirements	-Non-real-time -Response must be consistent -High throughput is demanded -High delay and jitter may be acceptable	-Real-time -Response is time-critical -Modest throughput is acceptable -High delay and/or jitter is not acceptable
Availability Requirements	-Responses such as rebooting are acceptable -Availability deficiencies can often be tolerated, depending on the systems operational requirements	-Responses such as rebooting may not be acceptable -Availability requirements may necessitate redundant systems -Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing
Risk Management Requirements	-Data confidentiality and integrity is paramount -Fault tolerance is less important – momentary downtime is not a major risk -Major risk impact is delay of business operations	-Human safety and protection of the process are paramount -Fault tolerance is essential, momentary downtime may not be acceptable -Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment or production.
Architecture Security Focus	-Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets -Central server may require more protection	-Primary goal is to protect edge clients (e.g. field devices such as process controllers) -Protection of central server is also important
Unintended Consequences	-Security solutions are designed around typical IT systems	-Security tools must be tested (e.g., off-line on a comparable ICS) to ensure that they do not compromise normal ICS operation
Time-Critical Interaction	-Less critical emergency interaction -Tightly restricted access control can be implemented to the degree necessary for security	-Response to human and other emergency interaction is critical -Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
System Operation	-Systems are designed for use with typical operating systems -Upgrades are straightforward with the availability of automated deployment tools.	-Differing and possibly proprietary operating systems, often without security capabilities built in -Software changes must be carefully made, usually by software vendors, to accommodate specialized control algorithms and perhaps modified hardware
Resource Constraints	-Systems are specified with enough resources to support the addition of third-party applications such as security solutions	-Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities
Communications	-Standard communications protocols -Primary wired networks with some localized wireless capabilities -Typical IT networking practices	-Many proprietary and standard communication protocols -Several types of communications media used including dedicated wire and wireless (radio and satellite) -Networks are complex and sometimes require the expertise of control engineers
Change Management	-Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	-Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. -ICS outages often must be planned and scheduled days/weeks in advance. -ICS may use OS's that are no longer supported.
Managed Support	-Allow for diversified support styles	-Service support is usually via a single vendor
Component Lifetime	-Lifetime on the order of 3-5 years	-Lifetime on the order of 15-20 years
Access to Components	-Components are usually local and easy to access	-Components can be isolated, remote, and require extensive physical effort to gain access to them.