Subject: Open Meeting of the Commission on Enhancing National Cybersecurity – CA

SMRP Comments on Enhancing National Cybersecurity

The Society for Maintenance and Reliability Professionals (SMRP) appreciates the opportunity to comment to the Commission on strengthening cybersecurity in the digital economy. The maintenance and reliability of cybersecurity systems and critical infrastructure is essential to the security of our nation.

SMRP recommends that the Commission should focus on the promotion, development, and implementation of a strategy for evaluating the impact of the known as the Internet of Things (IoT) devices and systems as it pertains to cybersecurity and infrastructure for small to large-sized business.

I. SMRP Introduction and Background

SMRP is an over 5,000 member professional society formed in 1992 to develop and promote excellence in the maintenance, reliability, and physical asset management profession. SMRP members consist of engineers, operations managers, repair and reliability technicians, worksite and project planners, and other service providers. We are experts in specification, design, purchasing, installation, inspection, testing, maintaining, decommissioning, and asset disposal. SMRP members can help evaluate the impact of cybersecurity and cyberphysical impacts of critical physical assets.

Maintenance and reliability jobs are skilled positions that provide competitive advantages to the companies that have them. Companies with highly trained, certified engineers reap a variety of benefits, including lower operations and manufacturing costs, reduced onsite injury risks, reduced environmental risks, and increased net profits. Nearly every industry sector requires the services of maintenance, reliability, and physical asset management personnel, including energy, oil and gas, pharmaceuticals, automotive, government and military, petrochemical, education, and commercial. Our ranks are made up of senior reliability managers from such companies as Cargill, BP, General Electric, General Motors, as well as utilities, government facilities, and the organizations that support them.

SMRP members are uniquely positioned to identify the impact of cybersecurity implementation on the reliability of the infrastructure, generation, and commercial / industrial end users. SMRP has developed enhanced tools that provide best practice metrics, benchmarking and reference materials for maintenance and reliability improvement. SMRP’s participation in global collaboration related to physical asset management, which is a framework for managing complex systems, includes recognized certifications from reliability programs to asset management, such as the ANSI-certified Certified Maintenance and Reliability Professional (CMRP) as well as the Certified Maintenance and Reliability Technician (CMRT) and internationally organized Certified Asset Management Assessor (CAMA).
II. Cyberphysical and Cyberinformation Advancements through IoT Devices

With advances in cyberphysical and cyberinformation systems (known as the Internet of Things (IoT)), unparalleled opportunities for improved monitoring, operations, and reliability of systems have been made readily available to all aspects of personal, public, private, and commercial entities. However, through rapid advancement and deployment, significant cybersecurity issues and infrastructure vulnerabilities have arisen as organizations do not necessarily understand the impact of a full threat.

A majority of IoT systems are implemented as monitoring systems and related maintenance systems within organizations and via third party maintenance organizations. These have the possibility of producing weaknesses in information security (cyberinformation), which may include critical operational and financial information, and access to controls, which may include the ability to effect systems and infrastructure (cyberphysical). Specialized search engines, such as Shodan.io, can easily identify internet connected systems, including maintenance systems, which provide support for internet security professionals who are verifying the accessibility of their systems, as well as cybercriminals who are searching for vulnerable systems. A great many applications for all operating systems, such as those for supervisory control and data acquisition (SCADA) systems, are freely available that can access systems for remote monitoring and operation.

On November 15, 2013, a complex cyberattack was conducted on Target stores through credentials obtained from a third party HVAC service company. Once cybercriminals obtained access to a beachhead in the HVAC service company’s contractor billing, contract submission and project management system, they were then able to use information provided via the portal to access Target’s credit card terminals. From November 27 to December 18, 2013, cybercriminals gained access to over 110 million consumer credit cards via Target’s email system.

At the present time, there is little to no understanding of the impact of cybersecurity issues resulting from third party vendors or on small to medium-sized manufacturing facilities.

III. SMRP Cybersecurity Positions and Recommendations

It is SMRP’s position that while an emphasis on larger organizations is important for a last line of defense, preventing cyberattacks on small to medium-sized organizations, and those that provide services to large-sized organizations and critical infrastructure should be the main focus. It is SMRP’s belief that an understanding of threats through IoT devices, contractors and subcontractors, regardless of size, and the development of cyberdefense processes will further reduce the risk to the economy and infrastructure of the United States and its allies. SMRP recommends a federal study on cybersecurity issues related to small to large-sized businesses and related infrastructure and third party support vendors including reliability and maintenance contractors and IoT suppliers; and the development of a process, or processes, to vet third party vendor cybersecurity and vulnerabilities.

SMRP also recommends research into the potential threat through the first line of defense and the interconnectivity between companies, vendors, contractors and subcontractors with an overall goal to establish a cyberdefense strategy. This includes the evaluation of cyberinformation, cyberphysical systems and best practice methods to prevent infiltration and damage to the front-line organizations. In essence, this will have an additional
impact on improving security for small to medium-sized businesses while reducing the number of attacks on larger organizations. Because current business models for larger organizations include contracting services through smaller companies, this presents an inherent problem as smaller firms are more prone to cyberattacks and can inadvertently exploit sensitive information from larger organizations. As a result, SMRP also recommends including the development of a vetting process and identification of tested and secure IoT devices and related systems and software for potential vulnerabilities.

IV. Summary

The maintenance and reliability of cybersecurity systems and critical infrastructure is essential to the security of our nation. We need to better understand the threats posed through IoT devices, contractors and subcontractors in order to truly reduce the risk to the economy and infrastructure. SMRP believes in a sound cyber-defense strategy and that research into the potential threat through the first line of defense and the inter-connectivity between companies, vendors, contractors, and subcontractors is the first-step towards this goal.

Thank you for your consideration and please do not hesitate to contact me if you have any questions.

Sincerely,

John Ferraro
SMRP Government Relations Director
529 14th Street NW, Suite 750
Washington, DC 20045
Phone: 202-207-1121
Email: jferraro@smrp.org