AUTOMATION FEDERATION | *The Voice of Automation*

FOUNDING MEMBER

The International Society of Automation (ISA)

CHARTER MEMBERS

The Organization for Machine Automation and Control (OMAC)

Wireless Industrial Networking Alliance (WINA)

MEMBERS

The American Small Manufacturers Coalition (ASMC)

The Continental Automated Buildings Association (CABA)

The Control Systems Integrators Association (CSIA)

Electronics Technicians Association International (ETAI)

The Institution of Engineering and Technology (IET)

The Measurement, Control & Automation Association (MCAA)

The National Career Development Association (NCDA)

The National Council For Advanced Manufacturing (NACFAM)

Project Lead The Way (PLTW)

The Society for Automation, Instrumentation, Measurement and Control (SAIMC)

The Society of Manufacturing Engineers (SME)

The Society of Manufacturing Engineers (SME) Education Foundation

The Society of Women Engineers (SWE)

23 September 2015

To Whom It May Concern,

Attached the Automation Federation response to NISTIR 8074. We appreciate this opportunity to comment on this important effort.

Please let me know if you require additional information and we look for to receiving the final report.

Thank you,

Sincerely

Michael Marlowe
Managing Director

Response to NISTIR 8074

Enhancing national and economic security and public safety

The Automation Federation is pleased that NIST understands the key differentiators between IT systems and Industrial Control Systems (ICS) and that security for these two system types is very different. However we believe continuous efforts are required to ensure this message is not lost. Even in the report there are references to IT issues such as "protecting sensitive information" without similar references to ICS issues such as "environmental disaster", "loss of life" or "loss of production". Cyber incidents contributing to ICS failure in the defense sector can be extremely severe and widespread.

As the report identifies, while much work has already been done in the development of ISA/IEC62443, there is still more to do. AF believes that more resources need to be directed towards the development of the ISA/IEC62443 standards set. Key areas that should receive priority treatment are:

- Cyber incident management – IT cyber incident management procedures are relatively well understood. For ICS, the procedures are not so well understood, specifically what should critical infrastructure organizations do in the event of a cyber incident: Shutting down continuously operating plant has its own risks, commercial and safety, and careful consideration and consensus is required to identify scenarios and recommended courses of action.

- Security automation and continuous monitoring – As with incident management, IT security automation and monitoring is relatively well developed. Security automation and continuous monitoring is much more difficult to implement in ICS. Disruption of finely balanced network communications timing and the lack of in-depth understanding of industrial communications protocols are two major limiting factors that will need to be addressed before this security barrier is more widely used.

AF believes government can play an important part in helping to be resource for the continued development of the ISA/IEC62443 standard set.

Ensuring standards and assessment tools are technically sound

AF agrees with the report's statement, "When protecting sensitive information and networks, government agencies need to have a minimum level of assurance that a stated security claim is valid". We believe that while self-assurance is one option, where security is concerned this assurance should be provided by an independent, certified, third party. Organizations such as ISASecure provide this independent assurance for Industrial Control Systems and their components by validating against the requirements in ISA/IEC62443. AF believes that the ISASecure model should be used as a reference point for independent security assurance.

Facilitating international trade

ISA/IEC62443 is an international standard and is widely used in ICS deployments around the world. Worldwide companies such as ExxonMobil, Du Pont and Shell have embedded ISA/IEC62443 into their ICS cybersecurity programs.

AF currently helps bring together the major international oil & gas companies together under the LOGIIC umbrella, to develop cybersecurity practices and guidance. Work is underway to create an international automotive manufacturer's equivalent to LOGIIC, which AF will also coordinate.

Promoting innovation and competitiveness

AF believes wider recognition and adoption of third-party verification programs such as ISASecure will help foster international trade in certified products. Compliance against the existing ISA/IEC62443 standard set requires innovation in product development. As the standard set is enhanced, ongoing innovation will be required to ensure that the critical infrastructure is based on safe and secure solutions.