MxD 15-01-01	Category: Recurring Manufacturing
Title:	Assessing, Remediating, and Enhancing DFARS Cybersecurity Compliance in Factory Infrastructure
Completion Date:	2017-02-28
Project Team:	Imprimis Inc., Rocky Mountain Technology Alliance Inc., SPIRE Manufacturing Solutions LLC
Coordinator Contact:	Jim Henderson Jim.Henderson@imprimis-inc.com
For Additional Information:	If you are a member of MxD (formerly DMDII), go to https://portal.dmdii.org/. If you are not a member of MxD, contact Tyler Vizek (Tyler.Vizek@mxdusa.org).

Summary:

MxD requested proposals to develop a baseline understanding of costs, capabilities, and effectiveness of Department of Defense (DoD) required cybersecurity measures for factory operations, specifically those identified in DFARS 252.204-7012. This DFARS clause requires DoD contractors and subcontractors to incorporate established information security standards on their unclassified networks. MxD requested an evaluation of the efficacy of the DFARS requirements in the face of low-end cybersecurity threats in order to ensure the protection Controlled Unclassified Information (CUI). i2 partnered with an interdisciplinary team from SPIRE and National Cyber Exchange (NCX) (formerly Western Cyber Exchange) to address this problem using proven techniques, coupled with innovative solutions. Specifically, the i2-SPIRE-NCX solution is unique in its use of a refined Commercial-Off-The-Shelf (COTS) tool to speed and simplify compliance assessment efforts and to enable the Risk Management Framework (RMF) process, in its review of Multiple Controls-Based Standards, and by creating a customized DFARS-Enhanced Standard for MxD use.

The team analyzed an SMM's digital manufacturing operations, their compliance with DFARS requirements, helped remediate their systems and processes to comply, and then re-assessed their compliance to validate near-complete compliance. The team then conducted “white hat” penetration testing of their known-compliant system to validate the strength of the DFARS Cybersecurity Standards for the manufacturing environment. It then developed an enhanced cybersecurity baseline based upon the DFARS requirements, but which adds specific controls related to industrial control systems (ICS) and specifically, manufacturing. In the assessment process, i2 utilized the i2’s advanced assessment and compliance tool (i2ACT-800), which incorporates numerous cybersecurity standards and baselines, reduces cost and effort in the assessment process, and provides key reports validating compliance and forming the basis for a remediation plan.

i2 then broadened its analysis of compliance, costs, and capabilities by assessing 5 additional manufacturing companies across two regions; collecting lessons learned and trending information. Finally, i2 and NCX analyzed cybersecurity training requirements to support DFARS compliance in manufacturing, proposed recommended training or certification, and provided training to MxD members on cybersecurity standards and assessment.