**AM Cyber Working Group Problem Summary**

**For the DOD Guidebook**

**Framing the DOD-Level AM Guidebook**

***AM Cybersecurity***

Facilitator: Al Lowas, Dana Ellis, Adwoa Amofa

**Three Key Topics**

|  |  |  |  |
| --- | --- | --- | --- |
| Categories | Topic 1 | Topic 2 | Topic 3 |
| AM Machine-Level Cybersecurity Investigation | Cyber Threats: What types of attacks are expected against AM machines? | Risk Assessment: Identify cyber vulnerabilities in (sample) AM machine(s) | Best Practices: What additional controls or design changes are recommended? |
| AM Network-Level Cybersecurity Investigation | Risk/Threat Assessment: Based on machines’ risks, what security should an AM Network provide? | Usability: What inherent functions are needed on an AM Network (sharing files, updating firmware, etc)? | Suggested Designs: What network designs are best suited to providing AM usability & suitable security? |
| Advertising to AM Manufacturers the need for Cybersecurity to be Baked In | Identify Common AM Machine Cybersecurity Gaps | Identify Vendors willing to address AM Machine Cybersecurity Gaps in their designs | Identify methods to spread these improvements across the industry. |

**King for a Day**

***AM Cybersecurity***

**These represent objectives which we intend to solve through the topics above:**

|  |  |  |
| --- | --- | --- |
|  | Topic | Goal |
| AM Machine-Level Cybersecurity Investigation | Cyber Threats: What types of attacks are expected against AM machines? | Identify at an unclassified level the types of threats that exist to AM Cyber machines so that vendors may better design against those kinds of threats. |
| Risk Assessment: Identify cyber vulnerabilities in (sample) AM machine(s) | Classify these vulnerabilities as (a) essential to AM machine operation, (b) inherent in Industry 4.0 designs, or (c) solvable with design upgrades. These categories will drive machine best practices, network best practices, and possible cybersecurity policy changes. |
| Best Practices: What additional controls or design changes are recommended? | Identify specific common additional machine controls that vendors might use across many machines. Identify specific recommendations for policy changes. Identify opportunities for security technology research/ development. |
| AM Network-Level Cybersecurity Investigation | Risk/Threat Assessment: Based on machines’ risks, what security should an AM Network provide? | Develop essentially a set of network design requirements for an AM network. Note that these design requirements might also be expanded to be useful for any industry Advanced Manufacturing Network. |
| Usability: What inherent functions are needed on an AM Network (sharing files, updating firmware, etc)? |
| Suggested Designs: What network designs are best suited to providing AM usability & suitable security? | Most companies will not have the time to design networks from scratch; however, a “cookie cutter” design for all industry and Government would be (a) costly and (b) its own vulnerability via excessive standardization. Thus identify a set of design recommendations that companies and DOD organizations may use in efficiently developing their own AM network. |
| AM Manufacturers Bake In Cybersecurity | Identify Common AM Machine Cybersecurity Gaps | Based upon the machine-based study (above), distill common AM Machine cybersecurity gaps into a format that is presentable to general AM Machine producers. |
| Identify Vendors willing to address AM Machine Cybersecurity Gaps in their designs | Recognizing that AM Machine producers are experts in new AM technology (not necessarily cybersecurity), identify those willing to design-in (“bake in”) cybersecurity as a product differentiation feature to their product line. |
| Identify methods to spread these improvements across the industry. | Leverage the free market, industry buying power, and DOD Contracting processes to encourage more AM Machine manufacturers to design-in more cybersecurity over time. Note: This will have a first phase of ramping up to an acceptable level of cybersecurity, and a second phase of continually adjusting to meet evolving threats. |

**Framing the DOD-Level AM Guidebook**

***AM Cybersecurity***

**Guidebook Text:**

The OSD, Military Services, and Defense Agencies will:

1. Continue to study the progress of AM design and implementation to update cybersecurity guidance as necessary for both contracted (Defense Industrial Base) and in-house (e.g. Organic Industrial Base).
2. Conduct cybersecurity assessments, monitoring, and management of AM machines consistent with their policies for other advanced manufacturing equipment.
3. Connect AM machines to enclaves (or other networks) consistent with their policies for other advanced manufacturing equipment.
4. Endeavor to share AM machine and network security information to the maximum extent practicable in order to reduce duplicate cybersecurity effort.
5. Require that commercial producers of AM parts (for DOD weapons systems or for the DOD supply chain) comply with Cybersecurity Maturity Model Certification, that those contractors show progress toward including AM machines in their CMMC considerations, and that those contractors develop Operational Technology (Advanced Manufacturing) security policies consistent with CMMC.
6. Include AM Machine cybersecurity considerations in their strategies for purchasing and supporting AM Machines for organic use.
7. Support joint Industry-DOD working groups to mature each of the requirements above.

Reference: Risk Management Framework, Joint Staff Implementation Guidance