Compromised Additive Manufacturing Supply Chain Workshop June 16, 2021

University of Maryland

UNIVERSITY OF MARYLAND 1856

MChESS
Maryland Center of Excellence for Sustainment Sciences

calce

Funding for this project was provided by the National Science Foundation Division of Civil, Mechanical and Manufacturing Innovation (Grant No. CMMI2039958)

Compromised Additive Manufacturing Supply Chain Workshop

The potential widespread adoption of additive manufacturing (AM) technology represents a marked shift in the production value chain. This shift represents a transition from value residing within the physical parts and structures, built from traditional designs and fabricated using conventional manufacturing to systems and components produced via additive manufacturing processes, wherein the value resides in the digital technical designs themselves, e.g., technical data packages (TDPs).

While the ability to produce parts and structures anywhere there are appropriate facilities and personnel provides great flexibility in the production process, the increasing reliance on digital data creates new challenges and complications (and new opportunities for malicious actors). Breaches of the data systems exchanging proprietary technical data packages enable anyone with access to the data and the appropriate equipment, to manufacture copies of the proprietary parts or structures and steal the intellectual property associated with the data package. Moreover, with the advent of affordable laser scanners, parts can be more readily reverse engineered to replicate the geometry (form & fit), but not necessarily function. These compromised parts could, in turn, be introduced into the supply chain, either for financial gain or other malicious purposes, without the requisite production controls (materials and processes), testing, evaluation, and qualification, leading to potential safety and liability issues.

This Workshop focused on the unique issues posed by compromised AM parts and components and how they can be mitigated.

Workshop Details

The virtual Workshop was held on June 16, 2021, via ZoomGov. The workshop included the following six sessions:

- Introduction and Keynote Address
- AM Technical Data Package (TDP) Panel
- AM Counterfeit Vulnerability Panel
- AM Security Perspectives Panel
- Counterfeit AM Parts Detection Panel
- Wrap Up

The workshop had 131 "unique" participants with 212 total logins to the workshop. The workshop was recorded to assist in the production of this report (after which the recording was destroyed).

Organization of this Document

This document provides an overall workshop summary followed by summaries of the individual panels. This document follows the Chatham House Rule with redaction of individual names and organizational identifications.

Workshop Summary and Outlook

Peter Sandborn (UMD Engineering), Steve Trimberger

The NIST definition of compromise is: "Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred." [1]

NIST SP 800-60 [2] defines three security objectives for information and information systems, Table 1. Although these are not targeted specifically at additive manufacturing (or any other component manufacturing process or technology), they represent a convenient reference structure.

Table 1: Information and Information System Security Objectives [2]

Security Objective	FISMA Definition [3]	FIPS 199 Definition [4]
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"	A loss of confidentiality is the unauthorized disclosure of information.
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"	A loss of integrity is the unauthorized modification or destruction of information.
Availability	"Ensuring timely and reliable access to and use of information…"	A loss of availability is the disruption of access to or use of information or an information system.

In many respects, the confidentiality concerns with AM are the same as they are with any other type of component manufacturing, i.e., confidential information embedded in the TDP (technical data package) can be accessed by unauthorized entities, which is also true for conventional manufacturing. The unique attributes of AM compromise (and the need for potentially unique countermeasures) appear to focus primarily on Integrity and Availability.

Similarities with Conventional Manufacturing

Before addressing differences between AM and conventionally manufactured components, it is useful to point out that there are significant similarities:

- Design
- Transmission of the TDP to the manufacturing process
- Post-manufacturing activities involving the finished part (inventory management, assembly, and testing of the component to the system)
- The function of the deployed component in the system

Presumably, these similarities can be addressed by the same mechanisms used for conventionally manufactured components, though we may wish to add new concerns and constraints. Still, if the issues are similar, but we are not concerned about them with conventional manufacturing, perhaps we need to consider why we have not been unconcerned before yet become so now. If the concern is legitimate, effort should be directed toward the whole problem, not just the AM component. The specific concerns for compromise articulated in this workshop encompass the following:

- Design (libraries and tools)
  - Malware insertion
- Transmission to manufacturing (blueprint, CNC codes, AM code, production steps)
  - Tampering
  - Counterfeit
- During manufacturing (manufacturing process flows and steps)
  - Errors due to inexperience with unfamiliar technology
  - Feedstock issues
  - Insider threats
- Post manufacture (delivery of parts for assembly into systems)
  - Tampering
  - Counterfeit
- Deployed component/system (system falling into an adversary's hands)
  - Reverse engineering

Physical devices can be reverse engineered. Reverse engineering (RE) was cited as a concern with AM, but the process and the expected success rate of RE should be the same for both AM and traditional manufacturing. The confusion in some minds is not in the RE process, but in the replication task, which AM appears to make simpler.

ID included during manufacture as a post-processing step. A unique identifying mark may be added during manufacture or affixed/machined into the part afterward. This may be easier with AM, where the actual manufacture of the component can be altered more easily, or the ID may be embedded within the component (for example as part of the internal structure or within the feedstock materials) rather than stamped on the exterior where it could be altered.

Machines are machines. A driver file for a multi-DF CNC tool is not qualitatively different from the AM data file. Similar risks exist; similar protections can be applied. If we do not worry about this for traditional manufacturing, why do we worry about it for AM (assuming maturity)?

Differences from Conventional Manufacturing

The differences between conventional manufacturing and AM appear to be primarily in the areas of:

- Transmission to manufacture
- Manufacturing processes

A physical device is represented as data. Some assurance can be had from general information security. As unique as this seems to AM, CNC instructions have the same property. Despite similarities with traditional machining, the flexibility of the AM machine makes data-representation protection a more attractive path for compromise.

- There may be additional types of PMI (product manufacturing information) that additive and casting may have that material removal does not have to contend with.
- There may be additional types of data that need to be defined for some AM technologies.
- The component specification should transition to a more functional specification versus the current material-oriented specification

Protection of the design. Encrypted data file prevents unauthorized copy. HMAC (hash-based message authentication code) assures provenance (anti-tamper) of the specification file. This also pertains to machining driver files. If we do not worry about it for traditional manufacturing, why are we worrying about it now?

Machines are not machines (yet). Today, no two AM machines produce the same component. This is problematic for highly qualified and certified critical systems. Our assumption is that this concern will become increasingly moot as AM printing technology matures. However, machines must potentially remain identical over very long periods of time (decades) for AM to become a useful technology for providing spare parts to critical systems in the future.

Protection of the device: Identity. The manufactured device may include a digital fingerprint, an intentionally created code, like a unique ID DR code built on the surface or internally (e.g., requiring X-ray to check). An ID can be applied in traditional manufacturing as well, but AM permits locating the ID internally, potentially hiding it from view. A watermark (or taggant) may pervade the component, making it impossible to erase. This code can be included using public-key cryptography to assure provenance.

Attractiveness to counterfeiters. For conventionally manufactured components for critical systems (particularly electronics), counterfeits become attractive because of shortages of legitimate components, rather than cost savings, i.e., the money saved on cheaper components is insignificant compared to the potential bad outcome of including a counterfeit component in a critical system. In the critical system space, counterfeiting is created by a lack of component availability. AM appears to undermines the value proposition of counterfeits because availability is assured (or it simply shifts the counterfeit value proposition from components to feedstock?).

Some compromises will not be malicious. Not all compromises (and compromise opportunities) stem from a malicious intent. Instead, they will result from poor manufacturing control, materials handling, machine setup, etc. (i.e., manufacturing mistakes, undisclosed material and process substitutions, etc.). Some of these issues will become moot as AM matures, however, this issue points out that manufacturing control/material handling/machine setup is a central challenge.

- These so-called "unintentional counterfeits" stem from compromising events that may (and often do) occur deeper in the supply chain than the final system manufacturer or sustainer has control over.
- Supply chain illumination must include feedstock (materials)

Distributed manufacturing makes manufacturing control challenging. With distributed manufacturing (distributed geographically and temporally), conventional manufacturing control potentially becomes more difficult.

Reliability. For AM, the manufacturing process has a significant impact on the microstructure of the material, which may not be present (or present in different ways) for conventional manufacturing.

AM compromise issues are not unique to AM. It should be noted that there are conventionally manufactured items already in use that live in a space that shares some AM unique compromise concerns, specifically FPGAs (field programmable gate arrays). These electronic devices are manufactured conventionally, and their functionality is customized via programming (potentially at or near the point of use). Like AM components, FPGAs share AM's integrity and availability concerns.

References

[1] NIST Special Publication 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001.

[2] NIST Special Publication 800-60, Volume 1 Revision 1, Volume 1: Guild for Mapping Types of Information and Information Systems to Security Categories, August 2008.

[3] 44 USSC, Sec. 3542

[4] Standards for Security Categorization of Federal Information and Information Systems, FIPS PUB 199, NIST, Feb 2004.

Summary of the AM Technical Data Package (TDP) Panel

Thomas Hedberg (UMD ARLIS), Ben Kassel (LMI)

The theme for this session is not that technical data for Additive Manufacturing is unique but that there are some unique considerations for technical data. Conventional and additive manufactured parts have similar requirements for shape data, configuration management, product, and manufacturing information (PMI), inspection, in-situ sensor, material specification, and machine instructions. The differences appear the deeper you dive into the model. There may be additional types of PMI additive and casting may have that material removal does not have to contend with. There may be additional types of data that need to be defined for SLS than is necessary for FDM. The overall process is similar, and the technical data architecture can be shared but differences in processes need to be accommodated whether it is setting the speeds and feeds for a milling machine or changing laser wattage and sintering times for a specific additive process. Whether it is controlling the tool changer and multiple heads on a 7-axis machine or controlling two nozzles with varied materials on an FDM tool.

PWI 52951, Additive Manufacturing—Data – Data Packages for AM Parts is a standard under development by International Standards Organization (ISO) Technical Committee 261 that provides guidance, methods, and models for developing a data package of a part created using additive manufacturing (AM) technologies. This Standard addresses the creation of the provenance of an additively manufactured part by identifying key information at distinct stages across a defined, production process. People who are interested to get involved with the standards effort should contact their home country's ISO Technical Advisory Group (TAG). People in the United States may contact Paul Witherall, paul.witherell@nist.gov, to get involved in developing the standard.

Technical Data for Additive Manufacturing parts has unique requirements due to several factors. The maturity level of AM, the unparalleled capability that AM provides for making parts in the field, and the fact that the manufacturing process has a significant impact on the microstructure of the material.

There are special concerns for AM electronics. Novel material sets, 3D complex form factors and additive processing conditions in AM electronics have complex effects on resulting microstructures, interfaces, defect structures and variability, that are very different from those seen in conventional (subtractive) planar electronics. TDPs need to keep sight of the effect of these variables on multiphysics, multiscale performance of AM electronics, both at start of life as well as the reliability over the entire life cycle. On-site AM repairs can alter the performance of electronics and TDPs need to specify qualification and acceptance standards for any such altered performance.

The U.S. Department of Defense (DoD) organizes a Digital Engineering Data and Modeling Working Group (DEDMWG) that focuses on capturing DoD stakeholder needs and requirements for technical data. The DEDMWG has an AM TDP subcommittee that specifically focuses on technical data for AM. People who are interested in getting more involved in 3D Model-Based Technical Data for additive manufacturing and becoming a member of the DEDMWG AM TDP subcommittee may contact John Schmelzle, john.schmelzle@navy.mil.

Summary of the AM Counterfeit Vulnerability Panel

William Lucyshyn (UMD Public Policy), Beverly McKeel (NSWC Crane)

The AM Counterfeit Vulnerability Panel was moderated by Dr. Beverly McKeel, from the Naval Surface Warfare Center, Crane. The Panelist included Dr. Justin Rettaliata (Naval Sea Systems Command), Mr. Doug Palmer (Booz Allen Hamilton), Dr. Abdalla Nassar (Pennsylvania State University), and Dr. Carrie M. Bartsch (Air Force Research Laboratory). The panel had two principal objectives. The first was to agree on a definition for what a constituted a counterfeit AM part, as well as compromised and unauthorized counterfeit parts. The second was to examine the range of Additive Manufacturing (AM) vulnerabilities throughout the production cycle that could lead to counterfeit or compromised artifacts being produced.

During the discussion of definitions, there was a consensus that AM was considered as being no different than other manufacturing process. The panel defined a counterfeit AM component as "an unauthorized copy or substitute product that has been identified, marked, or altered to resemble a product without authority or the right to do so, with the intent to mislead, defraud, or imitate an original component." On the other hand, a compromised part was defined as one where the Technical Data Package (TDP) has been tampered with or changed.

When it came to unauthorized additive parts, the panel believed that one needs to focus on and consider the vendors. The vendors that are use must work through a qualification process and be certified to produce the specific type of component. When a vendor is non-conforming, or unauthorized, they could be producing parts that might not meet the required standards or requirements for use in the system, i.e., an unauthorized counterfeit.

There could also be what we could describe as an accidental counterfeit. With conventional manufacturing much of the ability to produce a part, is dependent on the skill of the technician. There is an art, a skill, to produce a part that will meet all its requirements. With AM that knowledge is captured in the digital file, but there is a reliance on a COTS infrastructure to produce it. As noted below, the hardware and or software may be changed or manipulated, and as a result produce a defective component unintentionally. Inadvertent defects, flaws, or mistakes are very possible during the AM production process. A panelist opined "I think it means that it's extremely easy to have an accidental counterfeit," since it is difficult to discern the intent behind the counterfeit.

The panel next moved on to the discussion of AM vulnerabilities. They began with an examination of why AM security is difficult in general. For example, when considering printing metal parts, "the physics behind the process is hard." The processes range in timescales from microseconds (time for microstructures develop) to weeks (to print large parts), and these processes must be synchronized and coordinated. The spatial scales that affect the material properties, or the part, range from nanometers all the way to meters. The number of individual steps involved is tremendous. For example, for something like a powder bed fusion part there are hundreds of thousands of individual laser strikes. Although not typically done, in theory one can assign an individual set of processing parameters for each one of those lasers strikes. Getting the physics right to produce an actual component is not trivial.

The panel then went on to review what they believe are the vulnerabilities inherent in the AM cycle.

Data Handling. AM processes are inherently data intensive, but the data handling in today's systems is very messy. The process starts with the CAD data being exported to something like an STL file[1]. This file then goes into what was described as “black box processing systems” that create the actual AM build path. These resultant files structures that are currently used are quite opaque. Upstream effects and errors can be amplified downstream and carry all the way through to the final part. With many of these systems, the actual build plan used to build up the component vector by vector, contour by contour, is not accessible to the end user. Once these instructions are sent to the computer, there is less and less visibility over the actual processing paths and parameters that are used to build up the component. The panel identified a variety of ways to introduce errors into the TDP. These included changing the allowances in tolerances; manipulating the build files to introduce a defect or void that could make the part fail prematurely, or fail, in a way that it is not supposed to; and finally, the models could be altered, distorting the geometry of the part so that the form, fit, and function would fail. If someone changes some of the parameters, it may be very difficult to know or be able to reconstruct what they did. Unless there is an external process monitoring system, there is no tangible way to verify the instructions that are fed into the printer. It is important, to capture all the data that is available during fabrication and test to facilitate the acceptance process and understand the any limitations.

One of the approaches discussed to help secure the data was to use digital repositories, where the data cannot be tampered with and kept safe.

Hardware. Much of the Subsystem hardware that is used on AM machines is commercial off the shelf (e.g., commercial scanner, commercial laser, commercial computer). These components are integrated to assemble the AM manufacturing system. Vulnerabilities that may exist in those hardware systems, some of which may or may not be known, will carry through. If an actor modifies the actual way the machine operates, the produced component may not meet the design requirements. However, the damage may not only be to the part. There can be damage to the AM system itself, to the facility, or to human life if these machines are modified in non-desirable ways, since many metal-powder bed fusion and energy deposition machines are essentially inert explosive devices. Security is not just about ensuring that the part is not counterfeit, or that the part meets a particular specification. It is also about ensuring that there is no severe damage done beyond the part.

Integrating the process. Building a high-quality part necessitates many things working together, at the same time. Anything that affects one of the process inputs will affect the end-product performance and quality. For example, if the power settings are not correct, if the geometry is inadequate, or any of the other potential issues that can occur. This introduces the possibility of accidental counterfeiting (inadvertent defects, flaws, or mistakes), as well as intentional introduction of errors. All the layers are involved in the production process must be considered and secured.

Post Processing. Many AM produced parts and components require post processing. Specifically, with metal parts post processing is almost always required. For example, the part may need to be heated or treated to remove it from the build plate, it may need to be machined or hand finished. Vulnerabilities that exist in those downstream processes can also affect the performance of the finished components.

Feedstock. Even before considering possible counterfeit feedstock, even legitimate feedstock can introduce errors. The AM supply chain is typically vertically integrated since the process virtually

[1] STL (Standard Tessellation Language) is a file format used in some CAD software.

takes “raw material almost directly into a finished product.” As a result, counterfeit feedstock is a real concern.

Therefore, it is important to know where the input materials were bought, but also verify that they were handled properly. Feedstock behavior and performance is a not function only of the intrinsic characteristics of the material, it is also a function of how the material is handled and maintained, there are numerous parameters that can be associated with feedstock material that can impact its performance.

When using AM to print electronic circuits, environmental factors such as temperature and humidity content can change how the inks print. There are also many continuity issues that different inks can cause with printing electronics. When using silver ink from two different manufacturers, even the same silver ink, they can print in different ways. As a result, one cannot replace ink for one manufacturer with the same ink from a second manufacturer, because the parameters are often changed, because the substrate adhesion changes, the thickness obtained changes, in the end affecting the quality of the print product. As a result, there are challenges with repeatability, reproducibility, and, unfortunately, many opportunities for counterfeit materials to come into play.

Conclusion

There was also discussion of approaches to help mitigate the vulnerabilities. A key point was made by one panelist, “Consider security in all of designs as you're working towards a mission requirement, think about the limits of the AM system and process.” The use of non-critical markers or embedded security features, that are not necessary for the parts function, should also be considered, as well as knowing the limits and characteristics of your printers. Then if the wrong printer, ink combination, or printer material combination is used, it may could be detected. Additionally, it will be critical that the vendors are qualified and certified to manufacture the components, to ensure and that the parts that are produced to the required specifications and standards.

There was also a point made that to increase the flexibility of AM, i.e., to move away from the detailed material specification currently used for AM components, since material specification tend to be very specific. A panelist noted that “It has to be this exact alloy of this exact material and if it's not that exact one, we can't accept it.” If another alloy that is stronger and lighter is developed, it cannot be used. A functional specification would provide the necessary flexibility to adopt the improved alloy.

Summary of the AM Security Perspectives Panel

Thomas Hedberg (UMD ARLIS), Mark Yampolskiy (Auburn) and Joshua Lubell (NIST)

The theme for this session was focused on identifying and discussing security concerns and risks unique to Additive Manufacturing. Risk may be defined as a function of the threats to a system, the system's vulnerabilities, and the consequences of realized threats leveraging the system's vulnerabilities over time. Impact of risk was "the elephant in the room" during this session. The panelists talked a lot about threats and vulnerabilities. But it is the potential consequence (impact) that should also keep people concerned with the security of AM. Threats are only one part of the overall risk profile. We must understand the other portions of the risk profile to best mitigate risk to AM systems.

The session started by exploring the question, "How do AM attack impacts differ from IT, other cyber-physical systems (CPS) scenarios?" The results of the discussion around this question pointed to a general agreement that the differences between impact in IT and CPS scenarios well understood, but the difference between attacks in AM and CPS in general are much less understood. Further, many system compromises are successful because victims neglected well-established best security practices. The community must distinguish between an initial compromise of a system and an AM-specific attack itself that uses the compromised system. But AM does offer an opportunity to provide the design with security measures against some types of threats but not all threats. For example, in applied crypto, security measures against one threat do not necessarily protect against another type of threat. In addition, many threats are non-malicious and can be traced to human error, wear-and-tear, defects, and other physical phenomena. However, security controls countering and preventing intentional attacks can protect from some unintended consequences.

A panelist suggested the most worrisome concerns are variability in process and materials, compromise of data, and failure of a critical part due to attack that misses quality assurance (QA) checks. Another panelist suggested the likely types of cyber-attack are malicious modification (in both process and data) and reverse engineering of build files to copy material properties. Yet another panelist highlighted the following types of attacks and defenses:

- Attacks: side-channel, direct sabotage, reverse engineering, counterfeit production
- Defenses: encryption, micro-structure fingerprinting, embedded authorization codes, security as a design constraint

Other concerns reported were that many manufacturers are not following cybersecurity guidance and attacks are not being reported timely, if at all. Data sharing is more difficult than in traditional IT/OT environments. Sharing data between different companies, or even between departments within same company, is difficult when dealing with AM because of non-security concerns such as intellectual property trade secrets and data rights.

The current state of readiness and/or preparedness for AM attacks is unclear. There is agreement that a strong focus on qualifying parts would help --- sort of a zero-trust approach to AM processes and output. For example, what if we thought we made a good part, but it failed? We could search for root causes, which could be human or technical error, or intentionally caused failures. The QA of AM-produced parts can also be done for different motivations. However, the motivations do not change what happened, but emphasizes need for finding root causes, and driving how to address the failures. Unintentional failures will be addressed differently than intentional failures, but both types of failures may be discoverable using the same AM process security methods.

Lastly, the cost and investment in security is a factor too. Security is more affordable for OEM or prime (i.e., large) manufacturers than for small and medium size manufacturers further down the supply chain. There is a need for better supply chain traceability, and better sharing of ideas and methods among stakeholders and between industry and government.

In closing, the latest trends in the AM security landscape were heighted as:

- More intentional (malicious) compromise
- Increased security awareness --- hardware security in particular
- Kinetic nature of security (unlike conventional IT security)
- Machine learning and image faking enabling new threats

Summary of the Counterfeit AM Parts Detection Panel

Diganta Das (UMD CALCE), Sharon Flank (InfraTrac)

The closing discussions used the following bulleted discussion points to highlight the core points from the panel.

- Can counterfeit AM parts be detected?
  - We need the definition first – the intent is hard to determine
  - Built-in taggants and features that can be detected using special tools
  - "Soviet Typewriter" of printers can help in identifying the culprits
  - Acceptance criteria and quality standards can help as a first step as counterfeiters may not produces parts to the required level
  - Material can be a feature to check first – effective only if the "inspector" knows what to look for
- Can AM parts be protected? (besides protection through taggants)
  - Overproduction control – file expiration, supervisory software, material control
  - Distributed ledger solutions or Blockchain can protect the data, and that is often the beginning of protecting the part

Typically, the counterfeit has to do with IP violation-patent, trademark copyright, and trade secret. Is there a body of knowledge to extend that definition to additive manufacturing? On this same topic, the question remains on the final arbiter in deciding whether an AM part is counterfeit. The line between counterfeit and generic can also be blurry; there may be a need to support products analogous to the automotive aftermarket. This conundrum brings back the definition of counterfeit, and we will need to address that in a future meeting. The industry needs to define the minimum part requirements standard for the part that is manufacture type independent to help define an AM part and identify a counterfeit. The digital requirements must capture all the characteristics including material, functional, physical, coating, corrosion, magnetic, stealth, etc.

The panel pondered the issues that make it complicated to apply the lessons from avoidance and detection of counterfeit electronic components. The industry stakeholders need to agree on effective methods to address these issues. Since the AM supply chain for a specific part is often separate and exclusive, such decisions may also be made at that level.

Overproduction appears to be the only method of counterfeiting AM parts as all excess production can be defined that way. What is the best to stop that controlling the use of the production file or controlling the material availability? Any method against over-production needs to consider that some parts can be produced defective and should be discarded and manufactured again.

It is necessary to determine if it is essential to inspect the components for counterfeit risk. Since the manufacturing is distributed, the inspection point may be separate from the production and distribution point. There is typically no traditional distribution chain to inject the counterfeit AM parts into supply, and post-production modification of the parts is not likely to be the method of counterfeiting. One option is to consider that quality testing is also used as a counterfeit detection method by cataloging the "defects" detected. Some of the defects can only be detected by precipitating failures. The "accelerated" tests to simulate wear quickly need to become part of the process.

In detecting counterfeit electronic parts, a risk-based test sequence is used to ensure that appropriate levels of tests are performed that can identify the appropriate defects. There is a need to identify and the risk sources for this purpose. If the concern regarding counterfeit AM becomes a concern, the cost and time benefits associated with AM may be lost. The tolerance for testing burden may be low in the production setup.

There is also a concern about what one may call “accidental” counterfeiting. The feedstock “recipe” gradually changes over time, and at some point, the material will be identified as different, raising a false positive. Long-term storage impacts on feedstock also need to be considered in this regard.

At this point, external taggants appear to be the only proposed method for physically tracking AM parts. At the production stage, does one need special printers to “infuse” the taggants? We need to make several policy-level determinations to make that process effective. Decisions need to be made about how much information is needed to be shared with “inspectors” to detect the taggants and what tools are needed. If you include the taggant information in the technical data package, that needs to be access-controlled so that the secrecy of the process is maintained. At this point, we cannot ascertain if the TDPs come with an inspection plan for part acceptance and that is a point of decision.

When no “taggants” are built-in, which is likely to be the case, what other tools can be used to track? In those cases, can one use signatures from a machine as a tracking tool? In that case, will the machine manufacturers be willing and able to share such signatures with the stakeholders? Such signature can also be used to track where the parts came from – allowing easier identification of the culprit?