

MEMORANDUM

From: Robert Templeman, NAVSEA Distinguished Engineer for Cybersecurity
Date: 12-Mar-22
Re: Methodology for *OTS Hardware Assurance Recommendations*

NSWC Crane specializes in high assurance hardware and has long-supported DoD and other customers in the deployment of commercial hardware. NSWC has developed, and is sharing, a framework for using OTS hardware in non-enterprise applications.

The targets for these recommendations include all non-enterprise applications of Off-the-Shelf hardware, which covers tactical systems, support systems (e.g., maintenance systems, media generation systems), and maintenance equipment (e.g., test measurement and diagnostic equipment, TMDE).

The deliverables for this effort includes the following standalone documents: *Off-the-Shelf Hardware Threat Catalog*, *Off-the-Shelf Hardware Assurance Recommendations*, *Off-the-Shelf Hardware Assurance Glossary*, and this memorandum which details the methodology that was used during the effort.

Our hope is that these deliverables can be used as a basis for updating requirements and processes in order to deploy the most secure and resilient systems using inherently risky commercial OTS hardware.

Acknowledgements

Key contributors to this effort include (in alphabetical order): Jacob Avooske, Nathaniel Husted, Adam Shull, Adam Wiggerhauser, and colleagues at the National Security Agency (NSA) that we cannot acknowledge directly by name. Great contributions were made by key leaders in the Joint Federated Assurance Center (JFAC) and the Trusted and Assured Microelectronics (TAM) program.

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

WHY IS THIS IMPORTANT?

We should all know Homer's story of the Trojan Horse that recounts an unsuccessful 10-year siege that the Greeks laid on the city of Troy. Seemingly defeated, the Greeks retreated leaving a gift for the Trojans - a wooden trophy meant to atone for the Greek desecration of a Trojan temple. The Trojans were skeptical, but they accepted the gift and brought it into their city. The Greeks that were hidden inside emerged and were able to attack Troy's soft underbelly. The ancient Trojan priest Laocoon said, "I fear the Greeks even bearing gifts¹."

Many organizations rightly air-gap critical systems from threatening networks and have insider threat programs to vet and control their personnel, yet comparatively little is done to address supply chain threats. Supply chain threats often depend on a special kind of access, but today's global market offers opportunities that our adversaries exploit.

While we publically distance ourselves from overt Chinese products like Huawei and ZTE, many "American brands" are now owned and/or controlled by our adversaries. We are *gifted* with affordable commercial hardware that allows integrators to develop systems faster and cheaper; this same gift can give our adversaries footholds *inside* our systems.

Cyberspace is a formally recognized warfighting domain with many engaged nations and a high operational tempo. The Defense Science Board published a report on cyber resiliency in 2013 concluding that our nation does face existential cyber threats that rely upon assured strategic deterrents². The report goes on to say that not all DoD systems can, or should, be resilient against all cyber threats, but strategic systems require the very highest levels of assurance.

Our work seeks to equip programs of record with a usable framework to continue the use of OTS hardware in a way that is secure and resilient.

OBJECTIVES

We undertook the effort with the following objectives:

- Provide a prescriptive approach for engineering systems that leverage commercial hardware that will better secure systems from threats and vulnerabilities inherent to the use of OTS hardware.
- Provide recommendations that are compatible with flow down requirements to the extent possible.
- Leverage all existing, and proven, best practices to the extent possible. Focus on alignment to resources available from the Joint Federated Assurance Center (JFAC).

¹ In Latin, *timeo Danaos et dona ferentes*. Virgil. Aeneid II.

² Defense Science Board report on Resilient Military Systems and the Advanced Cyber Threat. <https://dsb.cto.mil/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf>. Accessed 27NOV20.

MOTIVATING EXAMPLES

There are many motivating historical accounts that underscore the need for systems of import to make efforts to be secure and resilient in the face of threats that come from the use of OTS hardware. Some examples from open sources stand out:

- Declassified by the National Security Agency (NSA) in recent years³, the GUNMAN Project details NSA efforts to discover and recover from a supply chain attack where Soviet operatives compromised typewriters supplied to the US State Department for use in Moscow and Leningrad. These modified typewriters allowed the KGB to see all generated written correspondence *as it was generated!* It took eight years for the NSA to discover this, which might have only occurred because of a tip from France, who was compromised in a similar way. While this example is 40 years old, the GUNMAN Project has remarkable relevance today because: 1) the cost of similar attacks has been driven down significantly and 2) our adversaries have **many** more opportunities to deliver supply chain attacks given the reality of the OTS hardware supply chain and how these products are pressed into use.
- In 2019, Red Balloon Security published critical vulnerabilities that they discovered with Cisco networking gear⁴. This attack demonstrates that adversaries can completely bypass security controls on the 'most secure' Cisco Switches and Routers. Affected switches and routers are on the NSA National Information Assurance Partnership (NIAP) Product Compliance List for use in the DoD's most critical systems.
- In 2016, Chinese agents were sentenced for conspiring to insert counterfeit critical microelectronics in the US Navy supply chain⁵.
- In 2010, FBI Operation Network Raider resulted in more than 700 seizures of counterfeit Cisco network hardware with an estimated retail value of \$143M⁶.

When one considers classified (or otherwise undisclosed) reporting and the legion of possible attacks against OTS HW demonstrated by researchers, it becomes clear that programs cannot ignore the risks posed by the threat of adversaries that have the means and opportunity, needing only a motive to attempt an attack leveraging OTS HW that we purchase for our systems.

³ The GUNMAN Project. <https://www.cryptomuseum.com/covert/bugs/selectric/>. Accessed 21SEP20.

⁴ The researchers document the exploit here: <https://thrangrycat.com/> and Cisco references one vulnerability here: <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot>. Note that there are no workarounds from exploitation and the great number of Cisco devices are affected. Accessed 21SEP20.

⁵ Chinese chap in the clink for trying to swap US Navy FPGAs with fakes to beat export ban, 15 months for fishing chips. https://www.theregister.com/2016/11/07/us_navy_fpgas_thief/. Accessed 21SEP20.

⁶ Departments of Justice and Homeland Security Announce 30 Convictions, More Than \$143 Million in Seizures from Initiative Targeting Traffickers in Counterfeit Network Hardware <https://archives.fbi.gov/archives/news/pressrel/press-releases/departments-of-justice-and-homeland-security-announce-30-convictions-more-than-143-million-in-seizures-from-initiative-targeting-traffickers-in-counterfeit-network-hardware>. Accessed 21SEP20.

PRECEPTS

This body of work is organized around the following precepts:

1. *Be hard to target.* OTS HW threats generally come from the supply chain when adversaries seek to achieve effects in target systems. This is done when an adversary can access COTS HW at some point in the supply chain (e.g., design, manufacture, distribution, and maintenance). A precisely-controlled effect requires that the adversary have strong knowledge of the target system. A fundamental defense of supply chain threats is to make yourself harder to target. In the worst case, a well-resourced adversary has a complete understanding of a target system (e.g., via an exfiltrated technical data package) and has full access to OTS hardware that is necessary for a target's missions. In the best case where an adversary can compromise the supply chain for OTS hardware, this adversary has no knowledge of technical or operational details of their target's missions, or even that their OTS hardware is in use. In the *Off-the-Shelf Hardware Assurance Recommendations* document, we address this via countermeasures to manage **Targetability**.
2. *Know thyself.* This ancient aphorism is a first class precept for cybersecurity. We must seek to know what is in our systems, where our adversaries have touched our systems, whether our system is in the right configuration, when malicious activity is observable in our systems... this line of questioning is long. In the *Off-the-Shelf Hardware Assurance Recommendations* document, we make recommendations for understanding cyber **Terrain**, seeking to reduce uncertainty about vulnerable surface area. The factual situation today is that many commercial products are integrated in systems with little vetting; the state of the global supply chain can result in situations where our adversaries have visibility to parts of our systems, which are our blind spots. These black boxes hold potential unknown unknowns that range from latent exploitable defects to malicious functionality. The concept of *Key Cyber Terrain* is widely-used, which is derivative of *Key Terrain* defined in JP 2-01.3. We recommend Ed Talbot's 2011 work titled "Cybersecurity Challenges and Opportunities," which details cyber terrain and the varying degrees of comprehensiveness in practice⁷.
3. *Security must focus on outcome.* A tome can be written on this precept alone. Many organizations make futile efforts using costly compliance-focused frameworks where the amount of documentation and people involved are presented as a proxy for how secure a system is. There are countless examples of these 'secure systems' that are compromised, often with ease. Ultimately, whether or not your system sees mission success facing expected cyber threats is what matters. Our adversaries do not play by your rules and they violate your assumptions. These assumptions, which can be formally documented or tacit, might involve how we think an adversary will (or will not) attack a target and about how much adversaries know about targeted systems (see 'Security by Obscurity'). In the *Off-the-Shelf Hardware Assurance Recommendations* document, we make recommendations for **TTP** (training, tactics, and procedures) aligned to objectives

⁷ Cybersecurity Challenges and Opportunities, <https://www.acsac.org/2011/workshops/gtip/p-Talbot.pdf>. Accessed 1MAY21

for effective organizational security operations, the delivery of uncompromised systems, and deployment of systems that operate securely and resiliently meet mission needs.

4. *Tailor security strategies to the magnitude of the risks.* Many risk management frameworks and efforts are ‘risk management’ in name only, not accounting for the actual risks a target faces. The Risk Management Framework, as generally applied, is a prime example where a primitive classification scheme determines ‘required’ control sets. It is commonly said that there is an art and a science to cybersecurity⁸, both are often eschewed focusing on checklists to achieve compliance. Our objective is the proportional application of well-implemented security controls that are necessary and sufficient.

SURVEY OF APPROACHES TO COUNTER OTS HW THREATS

There are a number of existing approaches that intersect with OTS hardware security. Some of these are policies that program offices are beholden to while others are whitepapers that offer recommended frameworks. Supply chain risk management and the threats from using OTS hardware are not new; there is a rich body of work that we draw from. The following is a non-exhaustive listing of programs, policies, and publications with brief summaries:

- Committee on Foreign Investment in the United States (CFIUS) (1975) – CFIUS is an inter-agency committee that reviews the national security implications of foreign investments in U.S. companies or operations. CFIUS has historically focused on economic security concerns, but focus in recent years has turned to supply chain concerns. The Foreign Investment Risk Review Modernization Act of 2018 (FIRREA) will bolster CFIUS to better address the increased pace of foreign investment efforts in U.S. companies. While CFIUS actions intersect with vendors that provide commercial hardware to DOD, CFIUS is not something that program managers or those in the acquisition community can employ.
- Trade Agreements Act (TAA) of 1979 – The TAA requires that the U.S. Government may acquire only “U.S.-made or designated country end products.” Given the complexity of supply chains for OTS hardware and the numerous ways that products can be compromised, TAA-compliance in itself offers no assurance and can lead to a false sense of security. There are many examples of products deemed “U.S.-made” with minimal *transformation* having occurred in the U.S..
- Common Criteria Evaluation and Validation Scheme (CCEVS) / National Information Assurance Partnership (NIAP) (2009) – The NIAP Product Compliance List is a whitelist of commercial products that are vetted by independent certification labs using standards, *protection profiles*, managed by the NSA. The RMF control enhancement SA-4(7), *Acquisition Process | NIAP-Approved Protection Profiles*, is levied upon OTS HW in many critical systems. This program draws from Common Criteria requirements and can

⁸ A seminal cybersecurity textbook is Professor Matt Bishop's, “Computer Security Art and Science.” <https://www.oreilly.com/library/view/computer-security-art/9780134097145/>

attest to certain security properties of OTS hardware, but this approach has perverse economic characteristics and the protection profiles are not adequately comprehensive.

- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) (2012) – Establishes policies and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission-critical functions or components. The TSN introduces a useful criticality analysis, which can identify components that bear the most risk to PMs, but the policy is limited, in both its guidance and governance, in adequately managing supply chain risk.
- DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) (2014) – RMF dominates DoD efforts towards securing systems. Ultimately, the security of a system is seen in a binary way. If a system has an ATO it is deemed adequately secure and suitable for deployment. If it does not have an ATO, it is deemed as not secure. The baseline control set in DoD generally comes from CNSSI 1253, which inadequately addresses threats to OTS hardware. The *OTS Hardware Acceptance Plan Recommendations* augments RMF by defining actions that can be executed to engineer inherently more secure systems and to manage supply chain risk with hardware assurance capabilities.
- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations (2015) – This standard generally addresses supply chain, seeking to comprehensively manage tactical-to-strategic risk across three defined tiers: the organization, mission/business processes, and information systems. The standard is not used in practice within DoD programs. The standard amounts to an overlay of approximately 110 added controls and enhancements.
- Never Contract with the Enemy Act, NDAA 2015 Section 841 – Superficially, this law would seem to apply to OTS hardware contracting where the landscape is rife with offerings provide or influenced by our adversaries. In fact, this law is limited to contracting efforts that take place in deployed environments, outside the oversight of GSA and related regulation.
- State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation reports (MITRE, 2016 and 2017) - These reports enumerate software assurance capabilities, which can be drawn on for assurance of firmware, and other software, related to OTS hardware.
- Supply Chain Attacks and Resiliency Mitigations Guidance for System Security Engineers (MITRE, 2017) - This report explicitly builds on the aforementioned 2014 OSD *Supply Chain Attack Patterns* report, here focusing on MITRE's resilience approach espousing emphasis of cyber attack lifecycles. MITRE offers 44 high-level resilience approaches to mitigate the 41 attack patterns detailed in the OSD report. This report does use a germane running example to detail their approach.
- Cyber Supply Chain (Defense Science Board, 2017) - The scope of this report is limited to microelectronics, but is comprehensive in its assessment of risks stemming from supply chain threats and latent vulnerabilities. This report highlights the limitations of current Program Protection Plan (PPP) policy, which addresses acquisition efforts, but does not robustly continue efforts into sustainment phases for programs. The

sustainment phase of a system lifecycle includes baseline/configuration changes and changes within the operating environment, which can present emergent program protection needs. This report ultimately recommends more research investment into hardware assurance and PPPs for sustainment. Note that Appendix A of this document has a superb comprehensive formulation of assurance.

- Deliver Uncompromised (MITRE, 2018) - This report thoroughly explains threats that stem from the supply chain and issues related to national-level policies. This report includes many detailed recommendations targeting national-level policy and statutes. This report does not offer program managers much utility aside from describing the problem well.
- Federal Acquisition Security Council (2018) – The FASC is designed to provide an interagency process through which the government can address potential security threats posed by commercial technology and includes representatives from the Department of Homeland Security, the Department of Defense, the Office of Management and Budget, the General Services Administration, the Office of the Director of National Intelligence (ODNI), the Department of Justice and the Department of Commerce. The function of the FASC is to use a principled process to identify commercial products that meet criteria for removal or exclusion orders.
- Cybersecurity Maturity Model Certification (CMMC) (2021)– CMMC is an emerging information security standard and certification effort that was motivated by events that illuminated widespread non-compliance of security standards within the defense industrial base (DIB). CMMC is identified by some as a supply chain security effort, but it is important to note that the current v2.0 standard includes no practices (i.e., requirements) related to OTS HW threats.
- Building a Trusted ICT Supply Chain (Cyberspace Solarium Commission, 2020) - This report focuses on national-level policy and makes strategic recommendations, much like MITRE's Deliver Uncompromised report. This report offers no practical value for near-term needs to securely use OTS hardware in programs of record.
- Information Communications and Technology Risk Reduction Subcommittee Final Report (DHS, 2020) - This report assesses Information Communications and Technology procurement practices at the Department of Homeland Security, finding deficiencies in the procurement and use of commercial products for unclassified systems, not unlike DoD findings. The report outlines high-level recommendations similar to MITRE's *Deliver Uncompromised* report and the Cyberspace Solarium Commission report.

JFAC AND OTS HARDWARE

The Joint Federated Assurance Center (JFAC) was established as a resource to programs of record to help mitigate threats inherent to hardware and software. The JFAC is a young and maturing organization having begun receiving significant funding in FY17. Much of this framework draws from JFAC efforts at-large. We made a methodological decision to maintain commonality with the JFAC when possible, but this work diverges in that the JFAC focus has been largely on the pursuit of trusted microelectronics (i.e., targets at the atomicity of electronic components). Our OTS hardware work clearly deals with higher levels of assembly and requires that we face some added challenges, which include: the presence of *many* microelectronic components within the scope of one assessment, printed circuit board assemblies and their associated supply chains, an enormous number of integrators compared to the relatively small number of integrated circuit fabrication facilities, the introduction of widely-varying software types, and different distribution channels.

Securely and resiliently integrating OTS hardware in critical national defense systems remains an open problem. The US Government has a growing suite of useful capabilities to help meet the objective; this work is a promising approach to integrate flow-down requirements/processes and a number of proven approaches in a usable way.

INTEGRATION OF OTS HARDWARE ASSURANCE EFFORTS IN DOD PROGRAMS OF RECORD

This framework integrates with existing processes performed during DoD 5000 acquisition efforts. The framework presumes collaboration between contractor teams and government assurance laboratories.

The *Off-the-Shelf Hardware Assurance Recommendations* document includes 34 recommendations aligning with acquisition and systems engineering processes in six phases:

Phase 0: Requirements Generation - System/subsystem architecture and requirement definition will identify CIs and influence the scope of assurance efforts (e.g., Level of Assurance or LoA). Systems most dependent on, and susceptible to, potentially malicious HW require significant assurance efforts (eleven recommendations).

Phase 1: Survey – Identify candidate products that appear to satisfy HWCI C2 specification requirements and vet vendors. Select products for evaluation (one recommendation).

Phase 2: Evaluation – Conduct supplier assessment and review available/supplied information to inform selection of product(s) for qualification (2 recommendations)

Phase 3: Qualification – Validation of requirements (3 recommendations).

Phase 4: Production & Deployment – Procurement and acceptance testing (2 recommendations).

Phase 5: Operations & Support – (4 recommendations)

Twelve recommendations are not unique to individual phases and have general applicability.

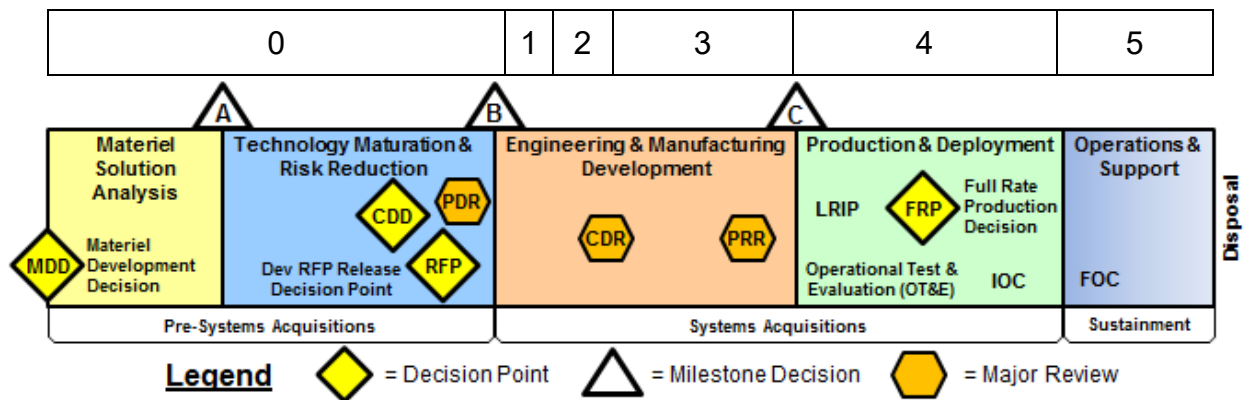


Figure 1: Approximate OTS HW Integration Phase Alignment to DoD 5000.02

UNCLASSIFIED

OFF-THE-SHELF HARDWARE THREAT CATALOG

DRAFT

UNCLASSIFIED

1.0 Introduction

This document catalogs categories of Hardware Assurance and general Supply Chain Threats that apply to Off-the-Shelf Hardware, OTS HW. This work was developed while collaborating with the National Security Agency (NSA) in support of the Joint Federated Assurance Center (JFAC). Our methodology seeks compatibility with JFAC approaches; this document extends JFAC work on trusted microelectronics to more complex levels of assembly, namely the general and broad category of commercial Off-the-Shelf Hardware. We use terms and definitions defined by the national assurance community; we recommend that users review the *Off-the-Shelf Hardware Assurance Glossary* for familiarization. Here we will define a few key terms that are fundamental to this document:

‘OTS HW’ – OTS HW or Off-the-Shelf Hardware describes commercially available hardware that includes information communications technology (ICT), test, measurement, and diagnostic equipment (TMDE), and other commercial hardware that has some degree of computing electronics therein. Examples include commercial power supplies, power conditioners, industrial control systems, portable computing devices, enterprise computing devices (e.g. servers/workstations), network appliances, storage devices (e.g., solid state drives or network attached storage), commercial bus/backplane computing, GPS receivers, printers, LCD displays, mice, keyboards, oscilloscopes, environmental monitoring equipment, test sets, etc.

‘platform’ – A platform refers to a specific device/product type or family of devices/products from a vendor. For example, Intel's Stratix 10 series of chips is an FPGA Platform and Cisco's Nexus 5000 series of network devices is an Ethernet Switch Platform.

‘system’ – A collection of related hardware and data comprising a final product or sub-component of a final product (i.e., what acquisition programs of record engineer and deliver). We seek to provide assurance to systems. A system may be a complete weapons system, or a sub-component of that system. When we discuss assurance, we are trying to protect the system from threats related to its specific use of OTS HW platforms.

This document details supply chain-related threats to commercial hardware, which are the basis for recommended countermeasures detailed in the *Off-the-Shelf Hardware Assurance Recommendations* document. We do not enumerate every specific technical method an attacker might employ (e.g., every known exploit that applies to a given network switch); instead we identify categories where common mitigation strategies and approaches will be necessary to use inherently risky commercial products for critical national defense functions. Threats originating from an adversary can compromise the operation of a system that leverages OTS HW by:

- Modifying its behavior from that which was intended
- Adding extraneous new behaviors
- Impeding or preventing its operation
- Degrading its operation or reliability

While this document does address issues of OTS HW quality or reliability in some circumstances, it does not provide general guidance on quality/reliability testing outside of the realm of detecting and preventing adversarial attacks. Programs with stringent or specific reliability requirements should not rely on assurance mitigations, but should instead conduct an appropriate level of testing to ensure proper operation of their systems.

2.0 Threat Descriptors

The work to catalog these threats began with an effort to gather data from all sources. These threats are inclusive of those commonly captured in open source reporting on COTS HW exploits, vulnerability disclosures, and related academic work. The threat characteristics were examined for commonalities and then summarized in nine broad categories, with titles deemed as *threat descriptors* (TDs):

- *TD1: Adversary inserts counterfeit materiel in a program/system/mission.* Example: In 2010, FBI Operation Network Raider resulted in more than 700 seizures of counterfeit Cisco network hardware with an estimated retail value of \$143M. Some amount of this materiel made its way to DoD programs¹.
- *TD2: Adversary inserts cloned materiel in a program/system/mission.* Clones are notably different from counterfeits. Counterfeit and authentic materiel share the same platform design and function, but differ in provenance. Cloned materiel purports to be authentic and have the same functionality, but has a different platform design. Example: FTDI makes USB components that are integral to many OTS HW devices; there have been a rife amount of cloned FTDI devices on the marketplace that replace a microprocessor programmed to act as a USB device, in lieu of an authentic FTDI ASIC. The motivation behind this example was to surreptitiously take market share from FTDI, but the same approach can be used to insert materiel in a supply chain with modified functionality².
- *TD3: Adversary uses access to program/system/mission information for targeting.* This threat category is broad. Programs provide sensitive information to vendors and distributors in the process of selecting hardware for use in a system. Certain OTS HW products afford vendors details on the end use of products, which can be used to target a program/system/mission. Some commercial networking products require a registration process where sensitive information is leaked and is easily accessible. Some OTS HW products require an Internet connection with a server for licensing, maintenance, or other purposes. This threat category can also include adversary access that would come in the form of regaining physical access to OTS HW targets that are sent out for maintenance, calibration, repair, or disposal.

¹ <https://archives.fbi.gov/archives/news/pressrel/press-releases/departments-of-justice-and-homeland-security-announce-30-convictions-more-than-143-million-in-seizures-from-initiative-targeting-traffickers-in-counterfeit-network-hardware>

² <https://www.zdnet.com/article/ftdi-admits-to-bricking-innocent-users-chips-in-silent-update/>

- TD4: Adversary exploits program/system/mission that experiences unwitting unauthorized change of configuration. Example: In the ideal case, assurance efforts include verification and validation on assets (i.e., targets) that are physically and logically identical to assets that will be used in operation (i.e., tight configuration control). In practice, programs experience significant variance of the configuration of deployed OTS HW. This comes from running changes to BOMs and from patches/updates. If a deviated configuration is less secure than the assured baseline, a system is rendered vulnerable. In this threat category, a system with poor configuration control can be exploited by known vulnerabilities.
- TD5: Adversary exploits failure of expressed or implied security features within materiel. Example: Thrangrycat is an attack that exploits poor implementation of a security monitor in Cisco network switches and routers. This failure of key security architecture makes 'secure' Cisco products less trustworthy than products in the platform that do not possess the exploitable security features³.
- TD6: Adversary exploits vulnerability latent within materiel. Example: There are a great number of 0-day (or 'zero day') vulnerabilities that affect OTS HW. This comes in the form of accidental defects that can be exploited and features that are exploitable for malicious effects (e.g., undocumented test modes).
- TD7: Adversary inserts malicious materiel at the OEM/OCM or upstream in the supply chain (control/modification of baseline configuration). This threat category includes compromised 3rd Party IP. Example: Academic work in 2017 demonstrated an analog Trojan that was inserted into the design at fabrication time for a commercial microprocessor⁴.
- TD8: Adversary maliciously modifies materiel in the supply chain downstream of OEM/OCM (departure from OEM/OCM configuration). Example: The Bloomberg "Big Hack" report purports that a motherboard manufacturer added hardware Trojans to SuperMicro motherboards⁵.
- TD9: Adversary compromises assurance capability/efforts defeating countermeasures to selected threat categories. Example: A past DARPA analysis found that 1/3 of software vulnerabilities came from cybersecurity products (e.g., antivirus software). This general vulnerability stems from the fact that security application software suffers from the same rate of software defects as other categories of application software. It should be expected that software-based products used to assure OTS SW are similarly vulnerable.

³ <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot>

⁴ <https://web.eecs.umich.edu/~taustin/papers/OAKLAND16-a2attack.pdf>

⁵ <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>. Investigation by the US Government and the cybersecurity community concluded that the claims of insertion of malicious implants in SuperMicro had no basis (e.g., no evidence was made available), but it is important to note that this sort of attack is feasible.

3.0 Levels of Assurance (LoAs)

The National Security Agency developed a framework that defines three levels of hardware assurance that can be applied to any system, which includes one or more instances of OTS HW with the intention of mitigating the full spectrum of currently known classes of assurance threats originating from OTS HW. In order to define these levels, the scope of the threats must be understood. Threats are scored in the areas of:

- The full cost to implement the attack. Cost refers to the entire spectrum of resources required to carry out the respective threat. These costs can include personnel requirements, tooling, processes and funding. It also includes opportunity costs associated with the attack. This combined metric is a stand in for the likelihood of an attack in traditional risk management approaches. Specifically, it controls for the dynamic element of an adversary responding to individual mitigations.
- The significance and targetability of their outcomes, prioritizing mitigations where an adversary could achieve with reliable, high-utility behavior effects. This corresponds to the consequence axis within traditional risk management approaches. The introduction of “targetability” into this measure seeks to emphasize the increase in consequence as the adversary’s control over their own attack grows.

Graphed against these two axes, assurance threats are binned according to the level of assurance (LoA) at which they are first relevant as illustrated in Figure 1.

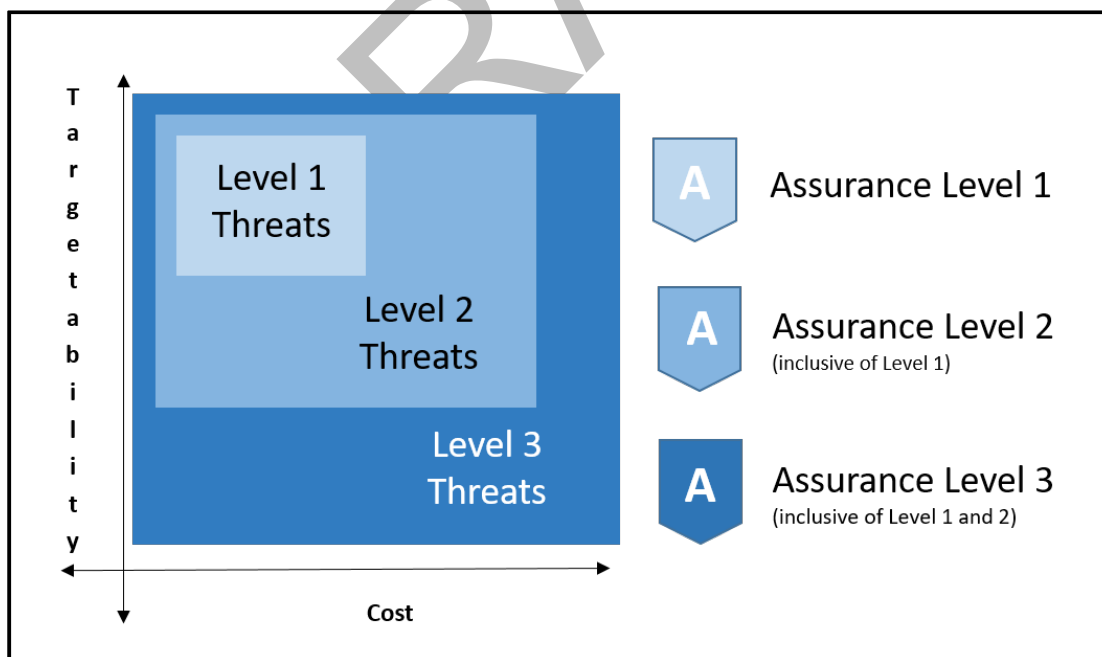


Figure 1: Cost vs Targetability / Threat vs Assurance

Three LoAs partition the capabilities and efforts that are required to counter threats. Each LoA is characterized by the threats that it counters and the assurance capabilities that are required:

- **LoA 1** - Threats that are inexpensive to implement but with high consequences.
- **LoA 2** - Threats in LoA 2 may achieve high consequence effects but with greater expense and investment. They may also include threats that are less targetable and most likely conducted for prepositioning, provided those effects can be achieved with a low or moderate costs.
- **LoA 3** - Threats that are very expensive to implement with unpredictable outcomes. Specifically, this covers threats that are feasible but may require extreme investment. It also covers threats that have marginal, or difficult to control effects.

The OTS HW threat descriptors were scored on criteria specified by the JFAC⁶: Access, Technology, Investment, and Targetability/Utility. The following table outlines the parameters for evaluating threats and identifying the corresponding Level of Assurance.

	LoA 1	LoA 2	LoA 3
	Threat Effort or Cost		
Access			
An available point of access	X	X	X
A difficult point of access		X	X
Multiple points of difficult access			X
Technology			
Existing public technology	X	X	X
Low Implementation Risk Technology		X	X
Technologically feasible			X
Investment			
Minimal investment of resources	X	X	X
A large multidisciplinary team		X	X
A nation scale and directed priority			X
	Threat Consequences or Impact		
Targetability			
Inherently targetable, controllable and high utility	X	X	X
Exist solely for pre-positioning		X	X
Blind attacks/ <i>Difficult to precisely target</i> or control the outcome			X

Table 1: LoA Criteria Matrix

⁶ A reference document is not yet available for distribution.

The scoring resulted in assigning the nine threat descriptors to the Level of Assurance at which they first become relevant. However, a particular threat category could have one attack that falls into LoA 1 and another into LoA 2. Further, a threat mitigation appropriate at LoA 1 might itself have vulnerabilities that make it unsuitable at LoA 2. As a result, different or additional mitigations might be required for LoA 2 than for LoA 1. The specifics of this are defined on a threat-by-threat basis and must be resolved by hardware assurance experts. In some cases, a cost effective mitigation might be sufficient for all LoAs. In others, a mitigation that is appropriate at LoA 1 may be superseded by a more complex mitigation at a higher LoA. Because of this, the JFAC best practices detailing valid mitigations are targeted at a specific Level of Assurance. The recommendations in this framework align to the JFAC approach.

In short, the overall process for building this catalog of threats is:



Figure 2: Threat Identification Process

The threat categories introduced in Section 2 focus specifically on assurance related threats; they are not inclusive of confidentiality, security or tamper related attacks except in areas where they overlap assurance concerns. **As a program utilizing OTS HW seeks to apply appropriate mitigations for a given Level of Assurance, that program will be expected to provide mitigations against the threat categories listed under the corresponding threat level.** The mitigations suggested by the JFAC best practices have been evaluated to mitigate those threats to the appropriate level. However, for higher LoAs, the program will need to address the same threats with higher LoA mitigations.

All programs/systems/missions of import, especially strategic programs, should anticipate targeting by adversaries. Supply chain attacks stemming from our nine listed threat categories should be expected even if a program adequately manages risk from external interfaces (e.g., networks) and insiders.

The LoA approach is finding general use in the assurance community and is a basis for the organization of capabilities to counter threats. LoA 1 threats are highly targetable and low cost. Mitigating assurance efforts can be conducted at the program office level (i.e., organic capability). LoA 2 assurance efforts will generally require support from specialized hardware assurance service providers. LoA 3 assurance efforts require highly advanced capabilities and are high cost (schedule and budget).

The threat categories addressed by this document are listed in Table 2 with the corresponding LoA(s) indicated. Note that TDs 1-7 each include diverse embodiments, but can be implemented in an achievable manner with high targetability. TDs 8 and 9 require a higher level of access which drives their assignment to LoA 2 and LoA 3.

#	Threat Description	LoA 1	LoA 2	LoA 3
TD 1	Adversary inserts counterfeit materiel in a program/system/mission	X	X	X
TD 2	Adversary inserts cloned materiel in a program/system/mission	X	X	X
TD 3	Adversary uses access to program/system/mission information for targeting	X	X	X
TD 4	Adversary exploits program/system/mission that experiences unwitting unauthorized change of configuration	X	X	X
TD 5	Adversary exploits failure of expressed or implied security features within materiel	X	X	X
TD 6	Adversary exploits vulnerability latent within materiel	X	X	X
TD 7	Adversary inserts malicious materiel at the OEM/OCM or upstream in the supply chain (control/modification of baseline configuration)	X	X	X
TD 8	Adversary maliciously modifies materiel in the supply chain downstream of OEM/OCM		X	X
TD 9	Adversary compromises assurance capability/efforts defeating countermeasures to selected threat categories		X	X

Table 2: Threat Description and LoA Matrix

Table 2 can be usefully interpreted as follows. First consider a hardware configuration item (HWCI) that resides within a system and its criticality on accomplishing a mission. The significance of this HWCI's role, both within the system and to accomplishing high-level objectives, determines the degree of threats that should be considered during risk management efforts; assurance efforts should be proportional.

These threat categories are not systematically mitigated by current DoD cybersecurity or supply chain risk management policy that flows down to program managers. While one *might* effectively implement RMF to counter these listed threat categories, the status quo is that programs accept or ignore residual risk due to unmitigated vulnerability to the nine threat categories that we list.

Our methodology memorandum details a great number of existing policies, standards, and efforts that one can use to manage risk, but there is no clear guidance on how to

UNCLASSIFIED

use the best elements of these together. Program managers can use the *Off-the-Shelf Hardware Assurance Recommendations* document for a prescriptive approach towards ensuring that a program/system/mission is secure and resilient when leveraging commercial off-the-shelf hardware.

DRAFT

UNCLASSIFIED

UNCLASSIFIED

OFF-THE-SHELF HARDWARE ASSURANCE RECOMMENDATIONS

DRAFT

UNCLASSIFIED

1. Introduction

This document provides recommendations for policies, processes, and requirements when integrating commercial Off-the-Shelf Hardware (OTS HW) in critical systems. OTS HW have been widely used with success since the mid-90's in many national defense programs with focus on mitigating quality and reliability gaps. These gaps arise from using consumer-grade electronics in physical environments that are very different from a home or office. Challenges like surviving mechanical shock, vibration, elevated operating temperatures, and interface interoperability were problems that we faced when using OTS HW. Our community developed solutions to these challenges and we have grown accustomed to the great benefits of leveraging OTS HW in our systems, but our adversaries now target our supply chains reducing the trustworthiness of OTS HW. This document describes our assessment of current policies, processes, and requirements and provides prescriptive recommendations. Implementation of these requirements will position a program to understand how supply chain threats inherent to OTS HW threaten our missions and to implement effective countermeasures.

We use terms and definitions defined by the national assurance community; we recommend that users review the *Off-the-Shelf Hardware Assurance Glossary* for familiarization. Here we will define a few key terms:

'OTS HW' – OTS HW or Off-the-Shelf Hardware describes commercially available hardware that includes ICT (information communications technology), TMDE (test, measurement, and diagnostic equipment), and other commercial hardware that has some degree of computing electronics therein. Examples include commercial power supplies, power conditioners, industrial control systems, portable computing devices, enterprise computing devices (e.g. servers/workstations), network appliances, storage devices (e.g., solid state drives or network attached storage), commercial bus/backplane computing, GPS receivers, printers, LCD displays, mice, keyboards, oscilloscopes, environmental monitoring equipment, test sets, etc.

'platform' – A platform refers to a specific device/product type or family of devices/products from a vendor. For example, Intel's Stratix 10 series of chips is an FPGA Platform and Cisco's Nexus 5000 series of network devices is an Ethernet switch platform.

'system' – A collection of related hardware and data comprising a final product or sub-component of a final product (i.e., what acquisition programs of record engineer and deliver). We seek to provide assurance to systems. A system may be a complete weapons system, or a sub-component of that system. When we discuss assurance, we are trying to protect the system from threats related to its specific use of OTS HW platforms.

Our recommendations focus on implementing system requirements via OTS HW for hardware configuration items (HWCIs). Our objective is to satisfy mission requirements despite threats posed to OTS HW. We understand the great demands placed on program managers and the challenging trade-spaces in which they operate. We base our recommendations on expected positive impact vs. cost (e.g., ROI). Our approach is to build a framework that unifies existing effective approaches, augmenting gaps with

added elements to sufficiently validate that our high assurance systems can face known threats when relying upon OTS HW.

We conducted a comprehensive assessment on policies, processes, and requirements that relate to the use of OTS HW in critical systems. The recommendations draw from successful efforts and approaches used within DoD, other government organizations, industry, and academia.

Mitigating supply chain threats is dependent upon general security operations to make yourself harder to target. Our recommendations assume prerequisite maturity in general security areas¹. Addressing general security programs is beyond our scope, but we offer recommendations to bolster general security efforts as needed to securely rely on OTS HW. We summarize these below:

- Insider Threat (IT) – We assume that a mature insider threat program is in place. This insider threat program covers malicious *and* unwitting threats and engages with national experts in counter intelligence to deny access to the organization's information and materiel.
- Information Security (INFOSEC) – We assume that information security operations are mature. This includes a well-defined security classification guide (SCG) informed by a threat model, and is accessible and understood by employees. Employees can demonstrate proficiency in the identification, marking, and handling of all levels of information.
- Operational Security (OPSEC) – We assume that an organization takes appropriate measures toward program protection via effective operational security. Organizations with mature OPSEC will minimize leakages of information on social media, via employees' LinkedIn accounts, through conversation with those outside of the organization and so on.

¹ Programs that do not have mature general security operations in the named areas should not disregard our recommendations, but should co-evolve, maturing general security alongside added assurance efforts.

- Industrial Security – A 2018 SECNAV report details how our nation’s adversaries are targeting the DIB to degrade our military advantages². Program protection and mission success depend on DIB partners adequately securing program equities. Industrial Security includes INFOSEC, IT, OPSEC and all of the other areas of security.

Our adversaries threaten our missions with their access to the supply chains of commercial products. This document is part of an engineering framework that integrates with existing development and deployment processes to leverage OTS HW in the execution and support of critical missions.

This framework focuses on mission outcome and supplements cybersecurity compliance efforts. Prescriptive tailoring guidance maximizes the affordability and value of assurance efforts. The recommendations in this document will help program managers identify when assurance is traded away and will reduce expensive and disruptive issues that surface after deployment.

2. Assessment of the Current State

Existing policy and guidance related to the deployment of OTS HW largely draws from the DoD 5000-series of documents and DFARS regulations. We do not exhaustively enumerate them here, but will summarize the efforts taken by typical programs during the selection and deployment of commercial hardware products.

Cybersecurity flow down requirements come from DoD requirements documents with RMF compliance being the ultimate cybersecurity objective for many programs of record. CNSSI 1253 defines the DoD baseline control set, which is a subset of NIST 800-53 that excludes most controls relevant to mitigating threats to OTS HW. Specifically, the *Systems and Services Acquisition* control family (i.e., ‘SA’ in rel 4) has a great number of effective and valuable controls/enhancements that are not used.

Hardware configuration items (HWCI) are typically identified following subsystem preliminary design review (SS-PDR). HWCI C2 specifications are generated from allocated subsystem requirements and relevant flowdown requirements. Security, trust, and assurance requirements are generally not present in C2 specifications, with occasional exceptions related to counterfeit materiel and National Information Assurance Partnership (NIAP)³.

² Secretary of the Navy Releases Cybersecurity Readiness Review Report
<https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=12268> (accessed 1SEP2020)

³ NIAP is responsible for Common Criteria Evaluation and Validation Scheme (CCEVS) validation body, which maintains a Product Compliant List (PCL) of OTS HW products that meet certain security standards called Protection Profiles (PPs). The NIAP approach offers some value as a rigorous validation of selected security properties, but this approach is not comprehensive in its rigor. There are numerous examples of compromised or exploited OTS HW that was on the NIAP PCL.

While system security engineering efforts should include assessments to identify necessary additional controls, Authority To Operate can generally be achieved by leveraging the minimum standard control set. When efforts *are* made to address risks of using commercial hardware in systems, there is a lack of rigor during control implementation and validation, which leads to vulnerable systems.

3. OTS HW Framework

There is a rich body of existing work addressing OTS HW security risks. We routinely see compromised OTS HW and effects on their users, which shows the need for a practical security framework. The *OTS Hardware Assurance Recommendations Methodology Memorandum* includes a summary of existing related efforts. The *Off-the-Shelf Hardware Threat Catalog* comprehensively considers threats to users of OTS HW and characterizes these using nine *threat descriptors* (TDs):

Identifier	Threat Description
TD1	Adversary inserts counterfeit materiel in a program/system/mission
TD2	Adversary inserts cloned materiel in a program/system/mission
TD3	Adversary uses access to program/system/mission information for targeting
TD4	Adversary exploits program/system/mission that experiences unwitting unauthorized change of configuration
TD5	Adversary exploits failure of expressed or implied security features within materiel
TD6	Adversary exploits vulnerability latent within materiel
TD7	Adversary maliciously modifies materiel at the OEM/OCM (control/modification of baseline configuration)
TD8	Adversary maliciously modifies materiel in the supply chain downstream of OEM/OCM
TD9	Adversary compromises assurance capability/efforts defeating countermeasures to selected threat categories

Table 1: Listing of OTS HW Threat Descriptors

The challenge for a program manager is understanding their risk through the lens of these threat descriptors and selecting the best countermeasures in the face of limited resources. The Holy Grail to secure OTS HW would be a prescriptive defined set of affordable controls (or countermeasures), that would mitigate risks when translated into requirements that are implemented and validated. We cannot expect to securely use OTS HW so easily. Coupling the diversity of DoD systems and the OTS HW ecosystem with continually evolving adversaries results in a complex risk environment that makes prescribed control set-based solutions unachievable.

Principles-focused cybersecurity approaches are a useful way to guide efforts to make systems secure and resilient. The DoD now requires that systems receive the Cyber Survivability Endorsement (CSE), which is part of the Survivability Key Performance Parameter (KPP) and relies upon ten Cyber Survivability Attributes (CSAs). The CSE approach applies CSAs to systems and can protect systems from some threats presented by OTS HW, but there is no intuitive application of CSAs directly to OTS HW.

Stated differently, there is no correspondence between the OTS HW Threat Descriptors and CSAs.

We recommend a tailoring framework that economically employs security courses of action that are necessary *and* sufficient. We do this using two dimensions 1) OTS HW Traits and 2) Levels of Assurance (LoAs).

3.1 OTS HW Traits

In biological contexts, traits are specific characteristics of an individual. A combination of genetic programming (design) *and* the individual's interaction with their environment determine one's traits, like hair color. Complex traits also determine whether individuals will be afflicted with diseases like diabetes or Parkinson's⁴.

In the same way, systems express traits determined by their design, implementation, and environment. We define the following OTS HW traits to inform the design and use of systems when implementing requirements with OTS HW:

3.1.1 Terrain

The cyberspace warfighting domain differs from other domains in that we design and build the terrain that we defend. The systems engineering process synthesizes cyberspace terrain. We sculpt terrain by coding individual lines of software and we add terrain designed by others. The use of OTS hardware, black boxes absent of design disclosure, are regions of our terrain that we cannot easily observe. Leveraging something like a commercial network switch might be key terrain that is defensible, or it could be key terrain already occupied by our adversary. We must shape terrain so that we can meet mission goals. Examples of shaping terrain include:

- The Principle of Least Privilege
- The Principle of Least Functionality
- Minimizing unknowns and uncertainty
- Configuration management/control
- Reconnaissance and surveillance

3.1.2 Targetability

Adversaries seek to achieve effects by attacking our systems any number of ways. Targetability affects where adversaries attack. An ideal target can be exploited by a precise effect with high utility (i.e., high consequence to us) that is controllable, difficult to attribute to the attacker, and has low cost. Targetability is reduced if the adversary's best effort to achieve an effect is not reliable, is not controllable, or is very high cost. In

⁴ <https://medicine.umich.edu/dept/human-genetics/complex-traits-diseases-0>.

the context of OTS HW, we concern ourselves with adversaries targeting our system from within the system via internal OTS HW. Examples of influencing targetability include:

- System/state observability
- Segmentation
- Mitigating targets of opportunity and criticality
- Deception
- Non-Persistence (i.e., denying adversaries from holding terrain)
- Maneuver

3.1.3 TTP (Training, Tactics, Procedures)

History is replete with examples in warfare where under-equipped fighters overwhelmingly defeat better-equipped adversaries. It is an incontrovertible truth that operational efficacy and efficiency are the victors' advantages. The TTP trait applies to systems, to both acquisition operations and during deployed use. In the context of OTS HW, the threats posed by using certain risky commercial devices can be mitigated by influencing the TTP trait:

- Secure communications
- Drills and other training
- War games for training and assessment
- Security operations
- Incident response
- Threat hunting

We developed these traits to be explicitly consistent with the operational warfighting community and to imbue an effective mental model for users. Our detailed recommendations are organized around influencing these traits while deploying OTS HW as part of managing cyber risk to mission.

3.2 Levels of Assurance (LoAs)⁵

The National Security Agency developed a framework that defines three levels of hardware assurance that can be applied to any system, which includes one or more instances of OTS HW with the intention of mitigating the full spectrum of currently known classes of assurance threats originating from OTS HW. One must understand the scope of threats to define the levels. We score threats in the areas of:

⁵ This subsection is a product of the JFAC and tailored for OTS HW.

- The full cost to implement the attack. Cost refers to the entire spectrum of resources required to carry out the respective threat. These costs can include personnel requirements, tooling, processes and funding. It also includes opportunity costs associated with the attack. This combined metric is a stand in for the likelihood⁶ of an attack in traditional risk management approaches. Specifically, it controls for the dynamic element of an adversary responding to individual mitigations. We must take into account the dynamic nature of cost and the tendency for attack costs to decrease over time.
- The significance and targetability of their outcomes, prioritizing mitigations where an adversary could achieve with reliable, high-utility behavior effects. This corresponds to the consequence axis within traditional risk management approaches. The introduction of “targetability” into this measure seeks to emphasize the increase in consequence as the adversary’s control over their own attack grows.

Graphed against these two axes, assurance threats are binned according to the level of assurance (LoA) at which they are first relevant as illustrated in Figure 1.

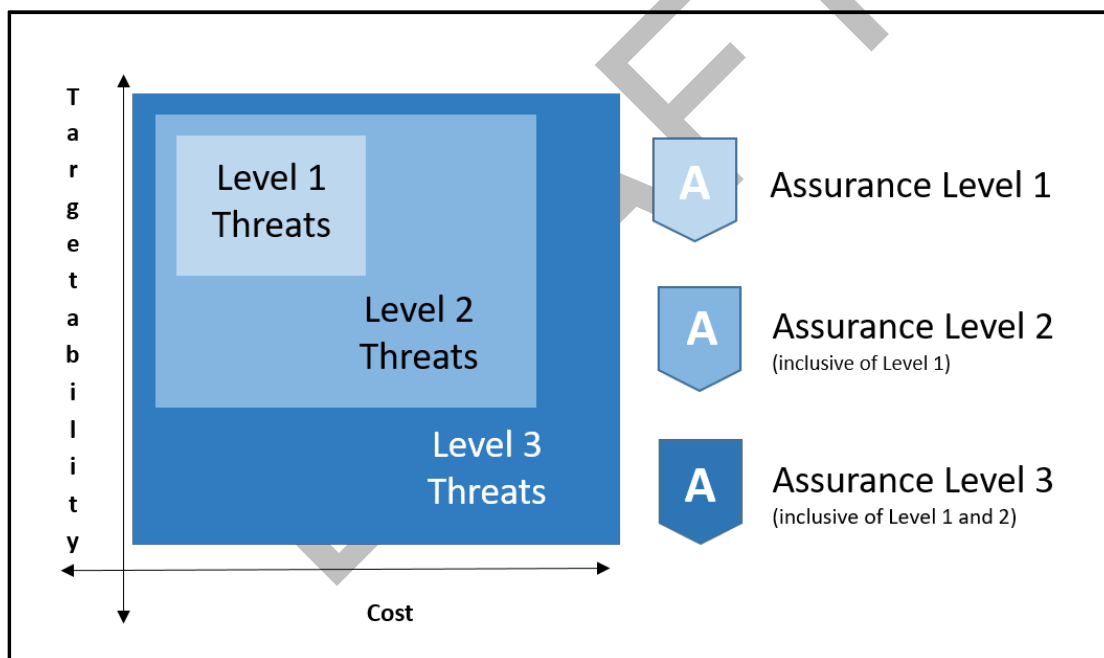


Figure 1: Cost vs Targetability / Threat vs Assurance

Three LoAs partition the levels of assurance capabilities and efforts that are required to counter threats. We characterize each LoA by the threats that it counters and the assurance capabilities that are required:

⁶ Likelihood as a dimension for gauging risk has little value in cybersecurity. In most cases, we only know that a risk event is 1) not yet realized and 2) not impossible ($0 < \text{Pr} < 1$). See the CIA’s paper by Sherman Kent: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays/6words.html>

- **LoA 1** - Threats that are inexpensive to implement but with high consequences.
- **LoA 2** - Threats in LoA 2 may achieve high consequence effects but with greater expense and investment. They may also include threats that are less targetable and most likely conducted for prepositioning, provided those effects can be achieved with a low or moderate costs.
- **LoA 3** - Threats that are very expensive to implement with unpredictable outcomes. Specifically, this covers threats that are feasible but may require extreme investment. It also covers threats that have marginal, or difficult to control effects.

The three LoAs address these threat categories beginning with the inexpensive and high consequence threats and continue across the spectrum. The mitigation requirements for each level are inclusive of the requirements of the previous levels and provide cascading protections. That is, a system that requires Level of Assurance 2 will provide mitigations to all threats that are relevant to LoA 2 and LoA 1. Accomplishing Assurance Level 3 requires a program to provide mitigations for Levels 1, 2, and 3.

Within this framework, a program must determine which Level of Assurance is appropriate for each instance of OTS HW (i.e., HWCI). That determination is dependent on two elements. The largest contributor to this determination is the criticality of the program, mission, system, subsystem, or configuration item. Missions/Programs where failure can be worked around using redundant⁷ systems and options in real time belong at LoA 1. Missions/Programs where the consequence of failure is dramatic, but which do not represent existential threats, belong in LoA 2. Missions/Programs whose failure represent an existential threat to the United States belong at LoA 3.

A second factor is the criticality of the HWCI to the system and mission. Some HWCI's may have their LoA reduced, because they are insufficiently critical to the system itself. One can determine a reduction in LoA only after a thoroughly conducted criticality analysis, which truly takes in to account all dependencies, including from the perspective of all trusted relationships. HWCI's within a system are often implicitly trusted and relied upon by other system elements in numerous ways. It is not sufficient to demonstrate that the role of a sub-system is less important. Its compromise must not allow an adversary access or influence over other, more critical functions.

There is a correspondence between LoAs and the criticality of a given component as identified by the *TSN Impact Level* (IL) using DoDI 5200.44. Table 2 shows the approximate mapping between LoAs and TSN Impact Level. Within this document, we will align recommendations with LoA levels, which more easily translate to available assurance capabilities in the National Security community.

⁷ A redundant system here must be a distinct system with a different design and supply chain. It is not intended to mean multiple physical instances of the same system design.

JFAC LoA	TSN Impact Level (IL) of component failure	
3	IL I	Total Mission Failure
2	IL II	Significant / Unacceptable Degradation
1	IL III	Partial/Acceptable
n/a ⁸	IL IV	Negligible compromise

Table 2: JFAC LoA / TSN Crosswalk

Table 2 can be practically applied by taking into account the Impact Level that is assessed for a given component; assurance efforts should be conducted at the corresponding LoA. Compensating mitigations might reduce required assurance efforts; foremost, reducing targetability at the system/subsystem levels.

The Joint Federated Assurance Center (JFAC) encompasses a network of government and industry labs that perform assurance functions for DoD. LoAs map to levels of capability within the JFAC.

- **LoA 1** – Assurance capabilities are generally accessible and may be implemented by qualified organizations throughout government and the Defense Industrial Base (DIB). The JFAC invests in and distributes a number of tools and resources to equip programs of record for LoA 1 assurance functions.
- **LoA 2** – Core JFAC labs perform assurance functions at this level using capabilities with limited access. These labs are focused on assurance functions for the larger community.
- **LoA 3** – NSWC Crane and the National Security Agency partner with selected affiliates for assurance capabilities at this level.

3.3 Intent for Recommendations

We developed a set of recommendations based on OTS HW threats and tailored on an assessment of current processes and practices. The recommendations assume an acceptance of the current state assessment and the OTS HW framework organized by Traits and JFAC LoAs.

Each recommendation maps to JFAC LoAs 1-3. LoA 1 recommendations should be implemented fully before considering LoA 2 and LoA 3 recommendations.

Principled implementation of the recommendations is necessary to mitigate known risks of relying on OTS HW in critical missions. We do not provide a fine-grained ordering for recommendations because each recommendation counters an adversary's ability to exploit OTS HW processes to compromise systems and missions.

⁸ Existing RMF-focused approaches may suffice for systems that have no impact to system or mission if completely compromised.

We detail each recommendation in Attachment 1 using the following fields:

- ID: A numeric identifier not related to priority or suggested order of implementation.
- Recommendation: A succinct description of the recommendation.
- Phase: * (all phases), 0 (requirements), 1, (survey), 2(evaluation), 3(qualification), 4(production/acceptance), 5 (operations/support). See the next page for details.
- Trait(s): OTS HW Traits (Terrain, Targetability, TTP) that the recommendation affects.
- Applies to: The target of the recommendation (i.e., system categorization, HWCI LoA, a named policy, etc).
- Performed by: Identifies the organization, group, or individual that implements the recommendation.
- Mitigates TDs: A listing of OTS HW Threat Descriptors that are mitigated by the recommendation.
- Guidance: Details for implementation.
- Rationale: A brief justification or rationale for the recommendation.
- Notes: Pointers to process documents and other information.

Additional attachments are referenced by individual recommendations. A listing of the individual recommendations is provided in Table 3 below.

Our recommendations align with acquisition and systems engineering processes and can be partitioned in six phases:

Phase 0: Requirements Generation - System/subsystem architecture and requirement definition will identify CIs and influence the scope of assurance efforts (e.g., LoA level). Systems most dependent on, and susceptible to, potentially malicious HW require significant assurance efforts (Recommendations #13, #14, #15, #16, #17, #18, #19, #20, #21, #22, #23).

Phase 1: Survey – Identify candidate products that appear to satisfy HWCI C2 specification requirements and vet vendors. Select products for evaluation (Recommendation #24).

Phase 2: Evaluation – Conduct supplier assessment and review available/supplied information to inform selection of product(s) for qualification (Recommendations #25, #27)

Phase 3: Qualification – Validation of requirements (Recommendations #26, #28, #29).

Phase 4: Production & Deployment – Procurement and acceptance testing (Recommendations #26, #30).

Phase 5: Operations & Support – (Recommendations #31, #32, #33, #34)

Recommendations #1-#12 are not unique to individual phases and have general applicability.

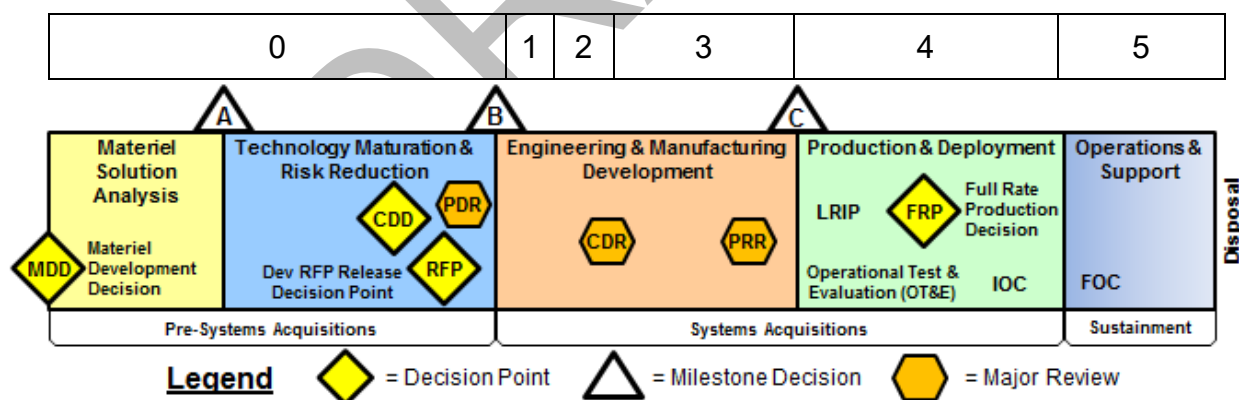


Figure 2: Approximate OTS HW Integration Phase Alignment to DoD 5000.02

ID	Recommendation
1	Apply the assurance framework to all uses of commercial hardware
2	Refrain from using likelihood-based assessments for assurance efforts
3	Integrate system security engineers (SSEs) on development teams
4	Seek anonymity when using strictly OTS (unmodified) products
5	Allocate compensating controls for reduced OPSEC when using modified products
6	Control and document exposure to OTS vendors and distributors
7	Leverage blind buys for evaluation, qualification, and production hardware
8	Use a cybersecurity assessment profile framework to select and interpret assessments
9	Add selected assurance-related artifacts to SETR milestone reviews
10	Ensure that use of OTS hardware will not spill information to vendors or other external programs
11	Include vulnerability notification agreements in contracts when possible
12	Considerations for Test, Monitoring, and Diagnostic Equipment (TMDE)
13	Conduct criticality analysis of systems at the granularity of HWCIs
14	Develop threat models for systems that document assumptions about adversaries
15	Conduct make/buy trade studies for IL I/II HWCIs prior to PDR
16	Allocate system requirement that OTS HW HWCIs cannot access system state
17	Allocate system requirements for functionality to detect indicators of compromise
18	Conduct low-cost system cyber table top (CTT) events prior to PDR and CDR
19	Identify low-assurance (LoA 1) and high-assurance (LoA 2/3) OTS HW HWCIs at PDR
20	Develop tailored HWCI assurance requirements using a threat tree for HWCIs considering TDs and threat intelligence (including mitigations)
21	Conduct gap analysis on Protection Profiles (PPs) when NIAP CCEVS is a requirement
22	Define and allocate assurance requirements for modified commercial products
23	Allocate and validate requirements for OTS HW configuration modification to include definition of privileged roles/users
24	Vet candidate OTS HW vendors for LoA 2/3 HWCIs using DoD resources
25	Leverage JFAC supplier assurance assessment for high assurance HWCIs
26	Procure and retain gold copy qualification and production assets for continuous assurance efforts
27	Leverage JFAC labs for assessment of OTS HW design documentation
28	Validate implementation of security requirements for high assurance HWCIs
29	Qualify two sources for LoA 3 HWCIs
30	Conduct a lifetime buy for LoA 2/3 HWCIs and validate configurations
31	Leverage tamper protection methods to preserve the integrity of OTS HW assets
32	Conduct failure analysis on failed assets
33	Conduct surveillance assessments of LoA 3 HWCIs
34	Operator cyber training

Table 3: Summary of recommendations; detailed in Attachment 1

4. Implementation Guidelines

- We suggest piloting/proofing recommendations on the selection/deployment of one HWCI before making program-wide process changes. Candidate pilot HWCI should be selected on the basis of generalizing results to all HWCI-types.
- While these recommendations can be applied tactically, on an ad-hoc basis, to any current effort that a PM faces, we strongly advise full integration of the full set of recommendations into a program's documentation and workflows.
- Use best-of-breed people, processes, and technologies for the implementation of recommendations, drawing from across the national security community and unrelated industry verticals (e.g., banking, finance, healthcare, insurance, media, and others).
- Rely on independent assessment and validation of implemented recommendations.
- We suggest a follow-up in one year to assess implementation.

Attachment 1: Recommendations

DRAFT

#1 - Apply the assurance framework to all uses of commercial hardware

Phase * Traits Terrain, Targetability, TTP

Applies to All commercial hardware

Performer PM, development team

Mitigates All TDs

Guidance

Use one authoritative process (e.g., a SOP based on this recommendations document) for all commercial hardware.

Rationale

Existing RMF-based approaches are insufficient to address the risk of using commercial hardware in DoD systems or supporting applications. This framework will comprehensively manage the risks inherent to the use of commercial hardware.

Notes

DRAFT

#2 - Refrain from using likelihood-based assessments for assurance efforts

Phase * Traits Terrain, Targetability, TTP

Applies to All assurance/cybersecurity/trust efforts

Performer PM, development team, assurance labs

Mitigates All TDs

Guidance

Risk matrices with ordinal categorical axes should be avoided (i.e., with categories across likelihood and consequence axes). The limitations of risk matrices is well-documented, while there is no principled basis for their use. See papers from Cox, Hubbard, and Thomas et al.^{9 10 11}.

The DoD BluGen assessment tool was developed for SSEs with the explicit goal to minimize subjectivity and effectively offers recommended courses of action absent likelihood estimations¹².

Rationale

Many individuals and organizations still use likelihood-based risks despite the uselessness. The problem stems from assuming sufficient data for frequentist-based likelihood estimates. If likelihoods are used, we strongly recommend the adoption of a Bayesian approach that seeks to estimate uncertainty related to the potential realization of events.

Hubbard and Seiersen's book *How to Measure Anything in Cybersecurity Risk* offers a proven and principled approach to manage risks.

Notes

⁹ Cox. "What's Wrong with Risk Matrices." <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6924.2008.01030.x>. Accessed 18MAY2021.

¹⁰ Hubbard and Evans. "Problems with Scoring Methods and Ordinal Scales in Risk Assessments." <https://ieeexplore.ieee.org/abstract/document/5464409/>. Accessed 18MAY2021.

¹¹ Thomas et al. "The Risk of Using Risk Matrices." <https://onepetro.org/EM/article-abstract/6/02/56/205611>. Accessed 18MAY2021.

¹² DODCAR Technology and Analytics. <https://intelshare.intelink.gov/sites/csarcop/layouts/15/start.aspx#/SitePages/Tools%20and%20Analytics.aspx>. Accessed 18MAY2021.

#3 - Integrate system security engineers (SSEs) on development teams

<u>Phase</u>	*	<u>Traits</u>	TTP
--------------	---	---------------	-----

<u>Applies to</u>	All CDTs and DDTs
-------------------	-------------------

<u>Performer</u>	PM
------------------	----

<u>Mitigates</u>	All TDs
------------------	---------

Guidance

Development teams should have organic expertise related to assurance and supply chain threats when integrating commercial hardware in a system. Qualified SSEs will be able to oversee implementation of an assurance framework, including all recommendations in this document.

The SSE should be familiar with organizations and capabilities that comprise the Joint Federated Assurance Center (JFAC) and should have experience with conducting system-level assessments, component-level cybersecurity assessments, and everything in between.

We recommend that SSEs are security specialists, but program generalists. A combination of deep and broad security experience across many programs brings to bear great value for programs. SSEs who are qualified engineers, by OPM or DAU standard, interface well with general system and acquisition engineers.

Rationale

Development teams do not typically have HW assurance expertise. RMF (IS) Information System Security Engineers (ISSEs) may have this expertise, but it is not common because RMF inadequately addresses hardware security.

Notes

DoDI 8500.01, *Cybersecurity*, mandates the integration of engineering and cybersecurity via SSEs, referencing CNSSI 4009, *National Information Assurance (IA) Glossary*, for definition. CNSSI 4009 points to NIST SP 800-37 Rev 1, *RMF for IS and Organizations*, for definition; this reference document was superseded by NIST SP 800-37 Rev 2; this document's definition of SSE functions is consistent with ours, but does not define qualifications. DoDI 8510.01, *RMF for DoD IT*, defines roles and responsibilities for executing RMF. Program Managers, IS Security Officers (ISSOs), and IS Security Managers (ISSMs) are responsible for ensuring that systems have an assigned ISSE, qualified IAW DoD 8570.01-M, *IA Workforce Improvement Program*.

In practice, ISSMs are often dual-hatted as RMF ISSEs. ISSEs are not formally assigned like ISSMs/ISSOs; ISSEs are informally identified and commonly qualified using SECNAV M-5239.2 under the "46, System Security Analyst" specialty area, which requires an approved degree **or** an industry certification: CASP, CAP, Security+ or SSCP. KSAs include "knowledge of systems engineering processes," but this is not a core KSA.

#4 - Seek anonymity when using strictly OTS (unmodified) products

<u>Phase</u>	*	<u>Traits</u>	Targetability
--------------	---	---------------	---------------

<u>Applies to</u>	All commercial hardware		
-------------------	-------------------------	--	--

<u>Performer</u>	Development team		
------------------	------------------	--	--

<u>Mitigates</u>	All TDs		
------------------	---------	--	--

Guidance

Maintain disciplined OPSEC for strictly OTS (i.e., non-modified) products.

Communications with vendors should be done in such a way that there is no attribution to PORs or POR systems. Take notice that that even if an individual development team member does not provide sensitive information during queries about products, affiliation via certain contractors or information on social media (e.g., LinkedIn) may give to deduction that a given commercial product will be used in a high-value system, which can aid targeting by adversaries.

Cleared defense contractors, or other vetted vendors, may justify an exception to this recommendation.

This recommendation applies to OPSEC during correspondence with vendors, to protecting information detailing that COTS products are used in POR systems, and to details about destinations where materiel will be shipped.

Rationale

Programs of record often have very high levels of exposure making them easy to target.

- Open source information can be used to learn roles and responsibilities of organizations.
- LinkedIn and other social network information can be used to identify roles and responsibilities of individuals.
- Unclassified information is not adequately protected in the defense industrial base.
- Some 'American' technology companies leverage production and logistics systems with contract manufacturers in China who drop ship products, whereby tying customer details to specific assets.

Strictly OTS products cannot be easily tailored to mitigate assurance risks and are typically black boxes.

Notes

While this explicitly applies in Phase 1, this OPSEC recommendation applies to all phases.

See related Recommendations #24 and #25.

#5 - Allocate compensating controls for reduced OPSEC when using modified products

<u>Phase</u>	*	<u>Traits</u> Terrain, Targetability
<u>Applies to</u>	LoA 2/3 HWCIs using commercial products	
<u>Performer</u>	Development team	
<u>Mitigates</u>	TD1, TD2, TD3, TD5, TD6, TD7, TD8	

Guidance

- Leverage the FBI Joint Counterintelligence Task Force (JITF) to compensate for inevitable exposure to vendors when tailoring products. This can be done via relationships with FBI field offices.
- Conduct supply chain analysis and illumination to determine third party IP that is used in candidate products.
- Include assurance provisions in the vendor contract to ensure that bills of materials and hashes for all embedded software are provided (see Recommendation #22).
- Use secure conveyance or other countermeasures to prevent downstream supply chain attacks (e.g., malicious insertion or other tampering while the HW is shipped from the vendor to the program custody).
- Validate HW and SW configuration of HWCIs upon acceptance and during operation (see Recommendation #33).
- Retain positive control over all HWCIs to prevent tampering. Unique LoA 3 (e.g., TSN IL I) hardware should be treated similarly to controlled cryptographic item (CCI) hardware.

Rationale

It is generally true that OTS hardware is not trustworthy and requires mitigating assurance efforts to achieve a usable level of trust at the system level. There are obvious limitations when using HW that is strictly off-the-shelf. However, tailored or modified commercial products open the door for valuable assurance efforts. In fact, these assurance efforts are necessary because modified commercial products are more targetable.

Notes

#6 - Control and document exposure to OTS vendors and distributors

<u>Phase</u>	*	<u>Traits</u>	Targetability
--------------	---	---------------	---------------

<u>Applies to</u>	All commercial hardware
-------------------	-------------------------

<u>Performer</u>	Development team
------------------	------------------

<u>Mitigates</u>	All TDs
------------------	---------

Guidance

Document all exposure to vendors retaining and segregating emails and using archivable communications modes whenever possible. Logging should include information on vendors (e.g., points of contact) and information on the exposure of the government team.

Rationale

A development team's communication with commercial hardware vendors often assumes some level of trust, which may or may not be founded. Recommendations #5 and #6 seek to reduce a program's exposure to vendors and to apply compensating controls when possible, but it is fundamentally useful for a program to know what their exposure to a given vendor is.

The recommendation has a twofold justification:

- Logging communications and other exposure to vendors can serve to bring increased awareness to interactions with vendors and to increase intentionality.
- Threat modeling is inherently difficult and based on many assumptions, to include what information our adversaries do or do not have. Documenting exposure aids threat modeling efforts (e.g., estimating what adversaries know about the program).

Notes

#7 - Leverage blind buys for evaluation, qualification, and production hardware

Phase * Traits Terrain, Targetability

Applies to All commercial hardware

Performer Development team

Mitigates TD1, TD2, TD8, TD9

Guidance

Use blind buy approaches so that vendors and distributors do not know that assets are being deployed to military systems.

See recommendation #10. A blind buy is less useful if acceptance of the hardware, or subsequent operation, reveals details of its use.

See recommendation #30. Budget for, and procure, a lifetime buy with enough spares to reduce dependencies (e.g., repair) on vendors and distributors.

Rationale

Security by obscurity is not a preferred approach, but programs must make intentional efforts to frustrate adversarial targeting if vulnerable commercial products must be used. Adversaries want to know exactly which hardware a program will use in a larger population of assets because adversaries generally seek precise effects that minimize collateral damage. This becomes increasingly important if an adversary has much knowledge of a system and how a platform device will be integrated.

Notes

#8 - Use a cybersecurity assessment profile framework to select and interpret assessments

Phase * Traits TTP

Applies to Development and operational efforts.

Performer Development team and the operational community

Mitigates All TDs

Guidance

Leverage the Cybersecurity Assessment Parameter Profile (CAPP) framework to select and use cybersecurity assessments. The notes section of this recommendation provides a link to this free resource. CAPP should be used to select individual assessment tools and as a lens to evaluate the results of an assessment. CAPP can be used to understand what a given assessment offers and limitations that exist.

- Advisory assessments are strongly recommended over strictly informational assessments. Cybersecurity assessments should be focused and prescriptive for PMs.
- It is self-evident that assessments should be conducted in a way that targets are seen as they will be seen by adversaries. Assessments based on models that are significantly different from production hardware can lead to compromised security and resilience.
- Quantitative assessments are perceived more attractively than qualitative assessments, but practitioners must exercise caution. Many quantitative assessments have little merit, either by design of the tool or how it is used.
- It is generally recommended to use standardized assessments over proprietary assessments, especially when the methodology is not disclosed. It is important to use an assessment with a sound methodology.

Rationale

The landscape of cybersecurity-related assessments is overwhelming. The US Government spends billions of dollars on cybersecurity assessments. There are countless numbers of assessment types and approaches. It is challenging to select what might be the best assessment tool and it is not obvious how to interpret finished assessment reports.

There are numerous backward-looking survey papers that provide summaries of assessment tools, but few frameworks to generally organize and understand assessments. The DoD Cybersecurity Assessment Parameter Profile (CAPP) framework, developed by NSWC Crane, characterizes and organizes assessments using a combination of substantive and procedural parameters.

Notes

The CAPP framework is an NSWC Crane product that was published to DTIC with Public Release Approval: <https://apps.dtic.mil/sti/citations/AD1049123>

#9 - Add selected assurance-related artifacts to SETR milestone reviews

<u>Phase</u>	*	<u>Traits</u> TTP
<u>Applies to</u>	Augment DoD5000 guidance	
<u>Performer</u>	SETR teams	
<u>Mitigates</u>	All TDs	

Guidance

In coordination with other recommendations, augment milestone review contents and/or packages as follows (this is a partial listing):

-Requirements Review (RR): System threat model and system mitigations, system assurance-related requirements, assessment of HWCIs and system state, indicators of compromise (IOC) requirements, Cyber Table Top assessment (CTT).

-Preliminary Design Review (PDR): Identification of HWCIs and respective LoA level, make/buy trades for LoA 2/3 HWCIs, identification of HwA requirements, CTT.

-Critical Design Review (CDR): Status on HWCI selection efforts (HWCI assurance/security requirement validation), CTT.

-Production Readiness Review (PRR): Assessment of validation of assurance requirements and recommended compensating TTP, CTT.

Rationale

This assurance framework was developed to integrate with existing development processes. It is self-evident that assurance elements will be added to milestone review packages.

Notes

*OTS HW assurance assessment to assess residual uncertainty and risk. See Recommendation #18.

It is especially important to exercise rigor with respect to requirements at all levels (system to HWCI). Recommendations #13-23 explicitly focus on assurance requirements (Phase 0) and will generate artifacts that are part of the technical design package and review contents/packages.

#10 - Ensure that use of OTS hardware will not spill information to vendors or other external programs

Phase * Traits Terrain, Targetability, TTP

Applies to All commercial hardware

Performer Development team, assurance labs

Mitigates All TDs

Guidance

Requirements should be allocated to C2 specifications ensuring that OTS hardware does not spill information during acceptance testing or during use. It is also important to ensure that there are no unintended external control opportunities for OTS hardware (e.g., functionality that allows remote access, control, or configuration modification). An obvious requirement could be that the configuration and operation of HWCIs has no external dependencies (e.g., access to a third party remote server).

Required interfaces should be documented in the C2 specification. Negative requirements should document forbidden interfaces to the extent that the HWCI only possesses the necessary interfaces. Compensating controls can work to disable or prevent the use of unneeded interfaces present on HWCIs (e.g., physical USB port blockers).

These requirements should be validated during qualification.

Rationale

Many commercial hardware products require interaction with the vendor or other external entity post-delivery. This comes in various forms:

- Network connection (persistent or situational). Some products must connect to the Internet to receive updates or to perform some other function. Some hardware products require persistent Internet connection for services that are hosted externally.
- Physical return to vendor or service provider. Products that require calibration, repair, or maintenance are sent out where there is opportunity for exfiltration of embedded information or tampering.
- Other cases. Some vendors require registration of products to 'activate' them. An example includes many Juniper networking products. In these cases, details on the end use of products are part of sensitive, and accessible, external databases.

Notes

#11 - Include vulnerability notification agreements in contracts when possible

<u>Phase</u>	*	<u>Traits</u> Terrain
<u>Applies to</u>	Selected commercial hardware	
<u>Performer</u>	Development and production teams	
<u>Mitigates</u>	TD1, TD2, TD5, TD6, TD7	

Guidance

Include in contracts a clause for mandatory timely notification of:

- All known vulnerabilities to include any that have not been publically disclosed. This includes vulnerabilities discovered internally and by external researchers.
- Compromises and potential compromises in the supply chain.

Strictly OTS hardware products may be exempt from this recommendation if the nature of the vendor or program OPSEC practices prevent such contracting.

Compliance with ISO/IEC 29147:2018, *Information Technology – Security Techniques – Vulnerability Disclosure*, might be a convenient reference point. Cisco provides a detailed public policy on their program, which adheres to the ISO/IEC standard: https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html.

Rationale

There are many cases when vendors have knowledge of product vulnerabilities that they do not publically disclose. This often occurs when researchers or users discover vulnerabilities and use a responsible disclosure process to notify vendors of vulnerabilities, allowing them time to develop mitigations before public notification. In some cases, mitigations can be developed and distributed in short order, but there are many cases where countermeasures take a long time to develop, or are even ignored. In the last case, vendors might use statutes to squelch attempts at public notification.

An emergent best practice is to use contracts to impose a requirement on vendors or distributors that notification will be provided when knowledge of a vulnerability emerges.

Notes

#12 - Considerations for Test, Monitoring, and Diagnostic Equipment (TMDE)

Phase * Traits Terrain, Targetability, TTP

Applies to TMDE

Performer Development team and operational community

Mitigates All TDs

Guidance

Leverage DoD-controlled calibration facilities when possible.

TMDE may, or may not, be subject to systems engineering processes, but many recommendations in this document apply:

#4: It may be unavoidable that TMDE be returned to a vendor or third party for calibration. Temporary removal of labels or markings that affiliate a piece of equipment to a critical system or program should be removed. The process should include proportional efforts to reduce targetability.

#10: Assess how the TMDE might spill information during its lifecycle.

#18: Conduct a CTT that addresses TMDE CONOPS focusing on interactions with mission systems. Specifically assess the potential for exfil of system information, the TMDE affecting the configuration of the system, and unintended interfaces with the system (e.g., covert channels). Factors include the type of interface (e.g., analog, digital, expressiveness), directionality of interfaces, frequency of use, calibration CONOPS, and exploitability of the TMDE.

#19: Most TMDE is LoA 1, but a criticality analysis should be conducted.

#20 and #28: A threat tree may be used during CTTs. Consider the degree to which the TMDE can be accessed internally. Countermeasures that leverage TMDE security functions should be independently validated.

#23, #26, #31: TMDE that has the potential to threaten the target system should have access controls in place and gold copies of the TMDE should be procured and stored.

Rationale

TMDE equipment is used in the production, maintenance, troubleshooting, and repair of systems. TMDE is almost entirely OTS HW that faces same threats as ICT, but has other considerations. Much TMDE requires recurring calibration by external organizations where tamper-evident labels are used to 'seal' products; breaking seals generally invalidates calibration.

TMDE CONOPS might serve as a vector to attack systems, yet many organizations do not apply any cybersecurity rigor to TMDE. Much TMDE escapes the application of RMF, but even when RMF is applied, the implemented control sets do not mitigate the OTS HW TDs. NSWC Crane has conducted assessments of individual TMDE, which provides amplifying information.

Notes

#13 – Conduct criticality analysis of systems at the granularity of HWCIIsPhase 0 Traits TerrainApplies to All systems that leverage commercial hardwarePerformer PMMitigates All TDsGuidance

Include a criticality assessment using the OSD TSN methodology (detailed in DoDI 5200.44) for impact level (IL) where:

IL I Total Mission Failure

IL II Significant / Unacceptable Degradation

IL III Partial/Acceptable

IL IV Negligible compromise

This assessment serves as a basis for HWCI assurance efforts. Use Table 2 in Section 3 to find the LoA that maps to IL for a given HWCI.

It is important to note that even IL I systems and subsystems can be engineered in such a way that individual components are categorized as IL IV. We recommend that systems be engineered for affordability that intentionally addresses trust. This includes leveraging authentication and confidentiality design patterns to enforce the principle of least privilege on networks and busses.

Rationale

Criticality analysis of system of system elements, related to mission, helps define the necessary level of rigor for cybersecurity efforts.

Notes

#14 - Develop threat models for systems that document assumptions about adversaries

Phase 0 Traits Terrain, Targetability, TTP

Applies to All systems/subsystems/hardware

Performer PM with LoA 2/3 assessment laboratories

Mitigates ALL

Guidance

A threat model should be developed and included in the Concept Review package. Attachment 3 contains a template for threat models. The threat model should be revisited, and updated as necessary, at each milestone review. CSTA-STD-010, *Cyber Risk Assessment Standard*, provides useful guidance on threat modelling, but we do not recommend using their likelihood-based quasi-quantified approach (see Recommendation #2).

Threat models should be considered at all abstraction layers within a system and will aid subsequent assessment efforts.

Programs should pursue threat intelligence from the JFAC: <https://jfac.navy.mil>. IRON GROVE is the intelligence support function for the Joint Federated Assurance Center (JFAC) and operates at the intersection of the counterintelligence (CI), foreign intelligence (FI), law enforcement (LE), and technical communities. IRON GROVE serves as a point for deconfliction and coordination while informing and enabling JFAC activities through actionable intelligence. You can request support by logging a ticket and selecting 'IRON GROVE' as a 'Department' and 'Counterintelligence Support' as a 'Request Category': <https://jfac.navy.mil/JFAC/hardware/ironGrove>.

Rationale

All programs and developers make cybersecurity-related assumptions about adversaries and threats. These assumptions manifest both explicitly and implicitly, but are rarely documented well. Attacking systems (i.e., offensive cyber) generally involves exploiting assumptions that developers make about systems.

Any rigorous cybersecurity capability includes the explicit definition of a threat model to detail assumptions about threats. This allows proportional tailoring of cybersecurity efforts.

Notes

Attachment 3 contains a template for documenting a threat model with knowledge or assumptions about adversaries.

#15 - Conduct make/buy trade studies for IL I/II HWCIs prior to PDR

<u>Phase</u>	0	<u>Traits</u>	Terrain, Targetability, TTP
<u>Applies to</u>	LoA 2/3 HWCIs		
<u>Performer</u>	SSEs and development teams with support from assurance laboratories		
<u>Mitigates</u>	All TDs		

Guidance

All LoA 2/3 HWCIs shall undergo a trade study to aid make/buy decisions. Factors in the trade include:

- Include assurance factors of Terrain, Targetability, and TTP in the trade space.
- Available HWCi requirements, which include flow down requirements from the system and subsystem(s).
- A cursory survey of the market for available products to satisfy requirements.
- A threat tree, or comparable cybersecurity assessment, to gauge threats and to identify all available countermeasures.

Off the shelf hardware will be used when there is an acceptable level of anticipated residual risk taking into account estimations of uncertainty.

Rationale

HWCIs may be implemented via strictly OTS products, modified commercial products, or via developmental items (internal or contracted externally). The selected approach is decided via a trade study. IL I /II HWCIs demand rigorous trade studies to balance assurance and cost.

Assurance may be unachievable for certain commercial products that perform critical roles.

Notes

#16 - Allocate system requirement that OTS HW HWCIs cannot access system state

Phase 0 Traits Terrain, Targetability

Applies to LoA 2/3 HWCIs

Performer SSE and development team with support from assurance laboratories

Mitigates TD2, TD3, TD4, TD5, TD6, TD7, TD8

Guidance

Targetability should be assessed from the concept phase in the development of systems where desirable triggers (from an adversary's perspective) are identified. System and subsystem requirements should be defined whereby untrusted system elements (e.g., HWCIs implemented by OTS HW) cannot be triggered to deliver precise effects.

Leverage independent informal architecture reviews or structured cyber tabletops to assess the targetability of implant-containing HWCIs in a system.

This recommendation is one in a family of requirements that can make a system inherently more secure to the point that the Impact Level of internal HWCIs may be reduced. This approach can serve to achieve resilience more economically.

Rationale

Knowledge about the state of a system is very valuable to adversaries and should be protected. Malicious payloads in disconnected systems require contextual information to precisely trigger effects and may leverage system state.

Programs whose documentation largely exists at the unclassified level should assume that adversaries have expertise knowledge related to system state and conditions, which will be used for exploitation if given the opportunity.

Systems can be designed to shield or obfuscate system state, which frustrates targetability by compromised HWCIs.

Notes

By *system state* we mean the combination of the current mode of system operation and contextual information that enables precise targeting of effects by adversaries. Absent remote access/control, system state affects targetability. Consider a kill-switch effect for a critical system; an adversary might want to trigger this only when the system is physically in a certain geographic region and when a specific operating mode is imminent. Required system state for this example includes the current physical system location and indicator(s) of system state.

#17 - Allocate system requirements for functionality to detect indicators of compromise

Phase 0 Traits Terrain, TTP

Applies to LoA 2/3 HWCIs

Performer SSE and development team with support from assurance labs

Mitigates TD2, TD3, TD4, TD5, TD6, TD7, TD8

Guidance

Additional detection capability should augment current data recording systems; the objective is to detect activity as far left in the kill chain as possible to enable response and recovery while minimizing the disruption of missions. OTS HW HWCIs are characterized during qualification, which serves as a baseline for detection during use.

Useful sensors would obviously monitor network traffic and also include sensors on other vulnerable system interfaces (e.g., USB), sensors to monitor power usage of HWCIs, and sensors to monitor potential covert channels (e.g., the RF environment).

The DARPA LADS (Leveraging the Analog Domain for Security) program offers approaches that might be considered¹³.

Detect/Response/Recover capabilities should be included during the concept phase of development and lead to requirements at the system, subsystem, and HCI levels. TTP should be used to explicitly include security in operations, which includes tailored cyber training for FTs and MTs.

Rationale

The NIST Cybersecurity Framework (CSF) is built upon a primitive set of functions that characterizes cybersecurity efforts: Identify, Protect, Detect, Respond, and Recover. Sufficient development and deployment efforts related to Identify and Protect could be enough to operate securely and resiliently, but in practice we know that systems are not adequately secured when they are initially deployed and will grow more vulnerable as time goes on. In fact, Identify and Protect efforts for systems are truly inadequate, which demands effective Detection, Response, and Recovery.

Commercial hardware products are various degrees of black boxes with contributions from many parties via the vast hardware and software elements that they contain. Identification and Protection is challenging at best. There is much talk about the risk assumed from exploitable latent vulnerabilities within commercial products. We do not recommend pursuing costly efforts to comprehensively discover latent vulnerabilities; investment in Detect/Response/Recover is more valuable.

Notes

¹³ LADS technologies are technology demonstrators that require maturation.

#18 - Conduct low-cost system cyber table top (CTT) events prior to PDR and CDR

<u>Phase</u>	0	<u>Traits</u>	Terrain, Targetability, TTP
<u>Applies to</u>	All systems/subsystems/hardware		
<u>Performer</u>	SSE-led with support from development team and assurance laboratories		
<u>Mitigates</u>	All TDs		
<u>Guidance</u>	Minimally conduct CTTs prior to PDR and CDR to inform requirement generation. Ideally, these CTTs would be conducted prior to all milestone reviews.		

Leveraging the language of CAPP (Recommendation #8), substantive parameters for CTTs should be advisory, have broad assessment targets (i.e., system level to include its environment), and use tailored standards focused on cyber risk to mission. Procedural parameters for CTTs should use standardized methodologies, rely on conceptual or modeled settings, use a mix of internal and external assessors in red (i.e., offensive) roles, and leverage qualitative analysis. CTTs should look at targets considering the traits and the TDs.

SSEs should lead CTT efforts composing small assessment teams with a mix of SMEs and including external expertise. CTTs can be scaled from hasty assessments done quickly with one SSE to large scale wargames. An appropriate CTT for a developmental milestone review should target 100 hours of labor.

Rationale

High-level cybersecurity requirements are easily defined during the development of systems, but coarse requirements must be refined and allocated to more fine-grained and implementable requirements as development progresses. Once requirements are defined, it is self-evident that principled approaches are necessary for implementation and validation. Compliance-focused cybersecurity efforts are not tailored to systems and often lead to inadequate requirements and deficient implementation/validation. This is especially true for assurance requirements.

Effective cybersecurity assessments comprehensively consider a target (at any stage from conception to a fielded system), its environment, and threats to recommend courses of action. CTTs are valuable assessments that can be conducted at any point in a system's lifecycle and can be scaled appropriately. These assessments provide effective ground truth on elements in the system that require attention/resources.

Notes

#19 - Identify low-assurance (LoA 1) and high-assurance (LoA 2/3) OTS HW HWCIs at PDR

<u>Phase</u>	0	<u>Traits</u>	Terrain, Targetability
<u>Applies to</u>	All systems		
<u>Performer</u>	Led by SSEs with support from development team and assurance labs		
<u>Mitigates</u>	All TDs		

Guidance

HWCIs and their corresponding LoAs will be defined at PDR using criticality analysis and system CTTs. Preceding efforts will be made to develop a system architecture to reduce costly assurance efforts for HWCIs.

Seek to develop systems such that HWCIs have criticality DoDI 5200.44 Impact Levels (ILs) of III or IV. This can be done by system and subsystem design that reduces dependence on HWCIs, and reduces vulnerability to attacking HWCIs. This can be accomplished using engineering approaches like the Cyber Survivability Endorsement (CSE) and using assessments (see Recommendation #18). Doing this reduces needed HWCI assurance efforts (i.e., HWCIs that are IL III/IV and require only LoA 1 assurance efforts).

A CTT (see Recommendation #18) and criticality analysis will determine appropriate LoAs for individual HWCIs.

Rationale

A key precept in cybersecurity is that countermeasures should correspond to threats with a proportionality relationship. Efforts to securely and resiliently use OTS HW in systems are tailored to how HWCIs are situated in systems.

Table 2 in Section 3.2 of this document details a crosswalk between criticality analysis and JFAC LoAs

Notes

Criticality analysis and Impact Levels (ILs) are defined in DoD 5200.44, Trusted Systems and Networks (TSN).

#20 - Develop tailored HWCI assurance requirements using a threat tree for HWCI considering TDs and threat intelligence (including mitigations)

Phase 0 Traits Terrain

Applies to All HWCI

Performer Led by SSE

Mitigates All TDs

Guidance

SSEs should construct threat trees to define C2 specification requirements based on threats and countermeasures. Assurance requirements will be identified by considering allocated system/subsystem requirements, HWCI interfaces, HWCI criticality, and threat intelligence.

Threats/mitigations will be labeled by LoA, which will determine assurance efforts. Assurance requirements may be critical or mitigatable. Certain requirements can be mitigated by subsystem/system or operationally via TTP.

Some guidelines:

- Avoid negative requirements that are difficult to validate.
- Each requirement should have a planned validation approach that will be included in qualification test plans. Resource requirements (schedule and cost) should be estimated.

Rationale

Current processes do not drive assurance requirements within HWCI requirements documents (i.e., C2 specifications).

Notes

There are various threat tree approaches. Adam Shostack's text on threat modeling is commonly used; the STRIDE framework can be replaced with the nine OTS HW threat categories.

The requirements review milestone should define each HWCI, system/subsystem requirements allocated to the HWCI, and describe significant interfaces.

#21 - Conduct gap analysis on Protection Profiles (PPs) when NIAP CCEVS is a requirement

Phase 0 Traits Terrain, Targetability, TTP

Applies to All OTS HW with NIAP CCEVS requirements

Performer SSE and LoA 2/3 assurance laboratories

Mitigates TD4, TD5, TD6

Guidance

Use the threat tree- and assessment-derived C2 specification assurance requirements to review PPs for coverage. The HWCI qualification test plan will include validation of requirements not satisfied by NIAP CCEVS testing.

Rationale

NIAP Protection Profiles use the Common Criteria as a basis, which is a general standard. While the Protection Profiles generally include some useful requirements and validation approaches, they are not comprehensive.

Case in point, the ThrangryCat exploitation of Cisco switches and routers took advantage of obvious gaps in PPs for network devices. In a compliance regime, programs will treat NIAP CCEVS requirements as a checkbox accepting unknown risk. Engineering-based approaches focused on cyber risk to mission will review PPs and test results to determine adequacy of coverage.

Notes

See NIST 800-53r4 SA-4(7)¹⁴

¹⁴ NIST SP 800-53 revision 5 reorganizes hardware security-relating controls, adding new controls and enhancements. The DoD baseline control sets, defined in CNSSI 1553, are still based on NIST SP 800-53r4.

#22 - Define and allocate assurance requirements for modified commercial products

Phase 0 Traits Terrain, Targetability, TTP

Applies to Selected LoA 2/3 HWCIs

Performer Development team

Mitigates TD1, TD2, TD3, TD7, TD8

Guidance

C2 specifications for modified commercial, and selected strictly OTS, hardware products should include requirements that vendors contractually provide artifacts to aid assurance efforts. This includes hardware and software bills of materials (BOMs) and hashes for all embedded binaries.

- This information should be cryptographically signed before transport to ensure integrity.
- This assumes a controlled configuration. Contract language should include details that updated information will be provided in the event of product design/configuration changes.

Rationale

Two questions must be addressed when using OTS HW platforms:

1. Is the platform adequately secure?
2. Does a given platform example have the expected physical and software configuration?

The latter question is much easier than the first to answer, especially when vendors provide supporting materials to aid assurance efforts, known as "acquire to verify." Absent support from vendors, assurance labs must document an exemplar's physical and logical design/configuration via construction analysis, physical configuration audits, and some degree of reverse engineering.

Notes

#23 - Allocate and validate requirements for OTS HW configuration modification to include definition of privileged roles/users

Phase 0 Traits Terrain, TTP

Applies to All commercial hardware

Performer Led by SSE with LoA 2/3 assurance laboratories

Mitigates TD4, TD5, TD6, TD8

Guidance

Conduct an assessment on the level of effort that is necessary to modify the configuration of candidate HWCIs that is commensurate with LoA and HWCI criticality.

- Consider open source exploits on the named platform and comparable platforms.
- Assess the presence of embedded binaries, vendor-provided update/patch methodologies, and debug ports.
- High assurance HWCIs may warrant assessment of firmware architectures.

The results of the assessment should include technical and TTP mitigations that will allow configuration management. The PM should initiate a governance plan that details TTP for configuration management that includes circumstances where changes in configuration are allowed.

Rationale

It does no good to validate the correct configuration of OTS hardware during acceptance testing if it can be later changed to the detriment of the mission.

The logical configuration of many commercial hardware products can be changed with little effort. This includes trivial modification of embedded data/executables or hardware that is configured by software via a user interface.

It is important to know the degree to which OTS HW can be modified and the level of effort that is required. Mitigations can be used to increase the cost of modification when necessary. TTP must identify and govern allowable circumstances for modification of OTS HW.

Notes

#24 - Vet candidate OTS HW vendors for LoA 2/3 HWCIs using DoD resources

<u>Phase</u>	1	<u>Traits</u>	Terrain, Targetability
<u>Applies to</u>	LoA 2/3 HWCIs implemented by commercial HW		
<u>Performer</u>	Various government organizations		
<u>Mitigates</u>	All TDs		

Guidance

Use DIA's DoD Supply Chain Risk Management (SCRM) Threat Analysis Center (TAC) to vet vendors of candidate HWCI products IAW DoDI 5240.24, *Counterintelligence Activities Supporting Research, Development, and Acquisition*. Use low risk vendors when possible.

Take note that policy like the Buy American Act (BAA), the Trade Agreements Act (TAA), or other policies that are used to assuage concerns about foreign influence have limited or no value. Due diligence is necessary to assess risk based on foreign influence. It is possible that *compensating controls can be used to reduce risk.

It is very important to implement other recommendations in this framework (e.g., Recommendation #4) in the event that an OTS HW product from a high-risk vendor must be used. The idea here is that when an inherently high-risk element is used within a system, compensating controls can reduce residual risk.

Rationale

Commercial hardware ecosystems are rife with vulnerabilities, threats, and exploits. This is partly due to competitive pressures to push minimally functional products to market while trading security away; this tradeoff brings lower prices. More concerning is the fact that many commercial vendors for hardware products are controlled or heavily influenced by foreign entities. These products may be aggressively marketed to national security programs whereby they can be integrated into systems that might be compromised before they are even deployed.

Due diligence is necessary to ensure that the riskiest vendors are not in consideration for HWCIs selection.

Notes

*Some companies assuage customer concerns by disclosing design details for independent assurance efforts (e.g., independent source code reviews).

#25 - Leverage JFAC supplier assurance assessment for high assurance HWCIs

<u>Phase</u>	2	<u>Traits</u>	Terrain
<u>Applies to</u>	LoA 2/3 HWCIs implemented by commercial HW		
<u>Performer</u>	Development team and LoA 2/3 assurance laboratories		
<u>Mitigates</u>	All TDs		

Guidance

Attachment 2 of this document contains an example questionnaire that can be used to engage with vendors. Note that this is an assessment that requires a cooperative vendor. Engagement of this nature with a vendor would be expected and appropriate when pursuing modified OTS hardware.

- Seek to have the questionnaire fielded by vendor employees that are qualified to provide responses.
- Note that many questionnaires are returned with vague or even inaccurate information. There is no effective criminal penalty for refusing to respond or for providing false answers.
- Note that the US Department of Commerce possesses special authorities to collect information from industry. These authorities levy specific criminal penalties for non-response or inaccurate answers. Circumstances that require non-attribution or difficult to obtain information might benefit from engagement with the Department of Commerce.

Rationale

Commercial hardware ecosystems are rife with vulnerabilities, threats, and exploits. This is partly due to competitive pressures to push minimally functional products to market while trading security away; this tradeoff brings lower prices. Recommendation #24 focused on the risk that comes from foreign influence to a vendor, but there are many other factors.

Due diligence is necessary to understand the security posture of hardware vendors and their offerings. While some information is available publically or from third parties, many cases require engaging directly with a vendor seeking answers to assurance-related questions.

Notes

#26 - Procure and retain gold copy qualification and production assets for continuous assurance efforts

Phase 3, 4 Traits Terrain

Applies to All commercial hardware

Performer Development team

Mitigates TD1, TD2, TD4, TD5, TD6, TD8, TD9

Guidance

Procure and retain exemplar examples of OTS HW HWCIs. Production examples should undergo acceptance testing with the retention of packing materials. A minimum of two assets from production are recommended. Evaluation and Qualification assets that do not undergo destructive testing should be retained.

These gold copy assets should be securely stored with physical protection in place to prevent tampering.

Rationale

Responding to cybersecurity incidents that involve hardware usually entails forensic analysis of some number of suspect devices. It is important to have access to 'gold standard,' or exemplar assets, that can be used as a basis for future comparison efforts, or to restore deployed assets to production baseline configurations.

Notes

#27 - Leverage JFAC labs for assessment of OTS HW design documentation

<u>Phase</u>	2	<u>Traits</u>	Terrain
<u>Applies to</u>	LoA 2/3 HWCIs implemented by commercial HW		
<u>Performer</u>	Development team and LoA 2/3 assurance laboratories		
<u>Mitigates</u>	All TDs		

Guidance

Review completeness of hardware documentation, identify high risk components, review embedded binaries, and provide overall risk assessment driven by C2 specification requirements.

Identify uncertainty (e.g., undocumented aspects of a potential HWCI implementation candidate) and mitigate accordingly (e.g., at the subsystem level or via TTP).

Rationale

While very few COTS vendors will disclose design information for their products, this is necessary for LoA 2/3 HWCIs; some vendors will oblige. There is a higher expectation of disclosure when dealing with modified COTS products.

DoD assurance laboratories should conduct assessment of design artifacts.

Notes

Design disclosure clauses can be included in contracts, but vendors may or may not supply the information that is needed. Some vendors simply lack granular info about their designs. Sometimes they are not forthcoming about what is in their designs; there are many ways that vendors can be non-cooperative. That said, some vendors provide excellent design disclosure. Note that the US Departments of Commerce and Treasury each have special authorities that can compel vendors to provide information. This is not easily leveraged, but certain cases warrant the use of these authorities where non-compliance results in criminal penalties.

#28 - Validate implementation of security requirements for high assurance HWCI

Phase 3 Traits Terrain, Targetability

Applies to LoA 2/3 HWCI

Performer LoA 2/3 assurance laboratories

Mitigates TD5, TD6

Guidance

Leverage qualified JFAC hardware assurance laboratories to validate the implementation of security- and assurance-related requirements in OTS HW products. These requirements will be included in HWCI C2 specifications. Validation will be detailed in HWCI evaluation or qualification test plans.

Rationale

Many cybersecurity incidents result from failures of security features, functions, or products. Research shows that security-related products do not have fewer vulnerabilities than products that do not relate to security.

Phase 0 recommendations will define system, subsystem, and HWCI security requirements that are required for mission assurance. Security requirements allocated to HWCI should be validated by a qualified independent assessor.

Notes

#29 - Qualify two sources for LoA 3 HWCIs

Phase 3 Traits Terrain, Targetability

Applies to LoA 3 HWCIs implemented by OTS HW

Performer Development team

Mitigates All TDs

Guidance

LoA 3 HWCIs should have more than one qualified source. This can be difficult to implement, clearly if only one source exists that meets requirements. Program managers must implement this considering their trade spaces, acknowledging the risk if they only have one qualified source for a LoA 3 CI.

Rationale

Hardware or software diversity in a system can frustrate an adversary's targeting efforts towards improving resilience. Having more than one qualified source of OTS hardware also aids recovery in the event that a qualified source must be removed from service. Systems that require the highest levels of assurance are high value targets where adversaries can use significant resources and long development times to field damaging effects.

Notes

#30 - Conduct a lifetime buy for LoA 2/3 HWCIs and validate configurationsPhase 4 Traits Terrain, TargetingApplies to LoA 2/3 HWCIsPerformer Development and production teamsMitigates All TDsGuidance

Leverage lifetime procurements for OTS HW products that take into account assets for initial fielding and spares. LoA 3 HWCIs should have acceptance testing to confirm the physical and logical configurations of 100% of assets. A-condition assets should be securely stored in such a way to prevent tampering.

Rationale

Risk from supply chain threats to hardware is a function of an adversary's access to a product's supply chain. Intuitively, reducing access generally reduces risk. One-time lot purchases of OTS HW products limit opportunities for downstream supply chain attacks, but also aid configuration management and eliminate obsolescence issues (provided spare quantities are reasonably estimated).

Notes

#31 - Leverage tamper protection methods to preserve the integrity of OTS HW assets

Phase 5 Traits Terrain, Targetability

Applies to LoA 2/3 HWCIs

Performer Development and production teams

Mitigates TD1, TD2, TD4, TD5, TD6, TD8

Guidance

Use protective technologies to defend against attempted tampering. These technologies can be used to prevent adversaries from gaining the physical access that is needed to compromise OTS HW products. The NSA's Protective Technologies group offers available products that include fasteners, tapes, and packaging.

The Protective Technologies group also offers training and materials to recognize tampering incidents.

Rationale

Attacks on hardware products can take place during transport, storage, or operation. It is important to protect the provenance of assets and to frustrate efforts to tamper with them.

Notes

#32 - Conduct failure analysis on failed assets

Phase 5 Traits Terrain, TTP

Applies to LoA 2/3 HWCIs

Performer SSE and assurance laboratories

Mitigates All TDs

Guidance

All failure reports should be reviewed by SSEs and correlated with system detection data (see Recommendation #17). Indications of suspicious failures should be investigated via forensic analysis by qualified assurance laboratories.

Preserving the state and condition of failed OTS HW assets is a best practice. Failed assets should be marked, segregated, and repackaged with tamper-evident products in the same manner as recommended in Recommendation #31.

Rationale

Perfect offensive cybersecurity effects can be achieved with no indication. Maybe there is the suggestion of a benign failure that is perceived as a reliability issue, which covers an underlying malicious attack. An important security objective is that there should be no silent failures. Programs and operators must be intentional to avoid unnoticed failures.

Notes

#33 - Conduct surveillance assessments of LoA 3 HWCIsPhase 5 Traits Terrain, TTPApplies to LoA 3 OTS HWPerformer Independent field inspection personnel and LoA 3 assurance laboratoriesMitigates All TDsGuidance

Conduct regular audits of fielded OTS HW to verify configuration. Field inspection is limited in scope, but can verify proper packaging and other observables.

Suspect materiel, nonconforming or tampered, should be investigated by a qualified assurance laboratory.

Rationale

Configuration management controls can fail to preserve CM. It is not uncommon to find non-conforming products in operational environments because of benign situations. High assurance systems should anticipate attempted malicious attacks. Surveillance activities, both in situ operationally and in a lab environment, can help validate the expected configuration of OTS HW.

Notes

#34 - Operator cyber training

Phase 5 Traits TTP
Applies to Ships force
Performer Training organizations and RIs
Mitigates All TDs

Guidance

Develop suitable curricula to train operators on cyber threats and cyber warfare.

Terminal

Learning Objectives (TLOs) should include:

- Knowledge and understanding of control system cybersecurity topics
- Understanding of related case studies and relevance to system(s) under use
- Knowledge and understanding of known adversary tradecraft
- Knowledge and understanding of indicators of compromise (IOC)
- Knowledge and understanding of response and recovery procedures for suspected cyber events

Rationale

Warfighters should be trained and equipped with knowledge, skills, and abilities to handle any threats that they will face. Certain military communities do this in a very structured and comprehensive way, namely pilots and the special operations community. In contrast, many watch standing roles are seen more banally, lacking the same level of preparation as a fighter pilot.

Operating warfighting systems of strategic importance demands the highest levels of preparation, which includes training on offensive cyber operations and anticipated threat landscapes.

Notes

Attachment 2: Vendor Questionnaire

The following questionnaire should be used to collect information to assess supply chain risk for vendors that serve national security customers. Evidence supporting responses reduce uncertainty when managing risk. Understand that asking the questions below may disclose an anticipated use of OTS HW in a sensitive application and can aid adversary targeting.

Manufacturer: Manufacture Legal Name

Part Number: Manufacturer Part or Model Number on Successive Rows

Serial Number: (if applicable for each device above)

Question 1: Where does the company primarily conduct hardware manufacturing operations related to the subject device? Are these operations contracted or organic? If the company utilizes contract manufacturing, please identify your primary contract partners and associated manufacturing sites.
Answer:
Question 2: What procurement controls does the company have in place to ensure that new and authentic microelectronics are procured from distributors authorized by the microelectronics device manufacturer?
Answer:
Question 3: When a microelectronic device required for production is discontinued, does the company utilized independent distribution to meet demand? If "yes", how does the company vet the independent distributor? And what testing and documentation are required from independent distributors to ensure the procurement of authentic product? Is any testing conducted internally to authenticate product?
Answer:
Question 4: Does the company issue product change notifications for significant manufacturing changes or discontinuances? How does the company determine if a configuration change is significant enough to warrant a notification? How is the customer made aware of these changes, and at what level is configuration data made available to the customer?
Answer:
Question 5: Does the company maintain lot traceability of all microelectronics from the component manufacturer to the serialized end item.
Answer:
Question 6: Does the company sell their products through an authorized distribution network? If so, who are your primary distributors, what requirements does the company impose on their authorized distributors, and how do you assess compliance?
Answer:

UNCLASSIFIED

Question 7: What security measures does the company employ at their organic and contract manufacturing facilities to insure that IP is protected, and that assemblies are not altered/accessed during the manufacturing process? How do you ensure compliance by contract manufacturers?
Answer:
Question 8: What cyber controls does the company implement to insure that critical design IP is protected from both extraction and manipulation?
Answer:
Question 9: Does the company ever outsource design of products to a third party? Was the design of the subject device outsourced? If so, who was the design partner?
Answer:
Question 10: Does the company assist users in validating that their product has proper hardware, software, and firmware configurations (e.g. Bill of Materials, Binary Hashes, etc)?
Answer:
Question 11: Does the company employ any protections to ensure that products are not intercepted or accessed/altered during transit? If so, please identify.
Answer:
Question 12: Does the company have any direct or indirect ownership interests related to a government or military? If so, please identify.
Answer:

UNCLASSIFIED

Attachment 3: Threat Model Template

THREAT MODEL [target identifier] [DDMMYYYY]

Objective:

The intent of this document is to capture details of a threat model to provide a context for assessments. It describes the target, its environment, factual threat information, and assumptions about threats.

Caveats:

1. Distribution of this threat model is strictly controlled by the originator.
2. To the extent possible avoid associations to programs and specific references to national defense systems.

Originator: Click or tap here to enter text.

Distribution list: Click or tap here to enter text.

Statement on sources for the threat model:

Does the customer have a comprehensive official threat model? Was the threat model developed by the originator alone? What sources does the threat model draw from? Where are assumptions made?

Click or tap here to enter text.

Target identifier:

Click or tap here to enter text.

Target background:

Click or tap here to enter text.

Target system background:

Click or tap here to enter text.

Prior target security efforts (e.g., certifications, accreditations, standards):

Click or tap here to enter text.

Assumed adversaries:

Click or tap here to enter text.

Adversary knowledge of target:

Click or tap here to enter text.

Adversary knowledge of target system (design and operation/use):

UNCLASSIFIED

Click or tap here to enter text.

Adversary knowledge of system POR:

Click or tap here to enter text.

Adversary physical access to target system:

Click or tap here to enter text.

Adversary remote access:

Click or tap here to enter text.

Supply chain threat:

Click or tap here to enter text.

Intended target interfaces:

Click or tap here to enter text.

Unintended target interfaces:

Click or tap here to enter text.

Unwitting insider threat:

Click or tap here to enter text.

Malicious insider threat:

Click or tap here to enter text.

DRAFT

Attachment 4: Assessment Criteria

The Federal Acquisition Security Council (FASC) uses the following ten non-exclusive criteria to evaluate sources and covered articles by analyzing available information¹⁵:

- (1) Functionality of the covered articles, including the source's access to data and information system privileges;
- (2) Security, authenticity, and integrity of covered articles and their supply and compilation chains, including for embedded, integrated, and bundled software;
- (3) The ability of the source to produce and deliver the covered articles as expected (i.e., supply chain assurance);
- (4) Ownership of, control of, or influence over the source or covered article(s) by a foreign government or parties owned or controlled by a foreign government, or other ties between the source and a foreign government, which may include the following considerations:
 - a. Whether the U.S. government has identified the country as a foreign adversary or country of special concern;
 - b. Whether the source or its component suppliers have headquarters, research, development, manufacturing, test, distribution, or service facilities or other operations in a foreign country, including a country of special concern or a foreign adversary;
 - c. Personal and professional ties between the source—including its officers, directors or similar officials, employees, consultants, or contractors— and any foreign government; and
 - d. Laws and regulations of any foreign country in which the source has headquarters, research development, manufacturing, testing, packaging, distribution, or service facilities or other operations.
- (5) Implications to national, homeland security, or critical functions associated with use of the source(s) or covered article(s);
- (6) Vulnerabilities of federal systems, programs, or facilities;
- (7) Capacity of the source or the U.S. Government to mitigate risks;
- (8) Credibility of, and confidence in available information used to formulate assessment(s) of risk associated with proceeding, with using alternatives, and/or with adopting range of mitigations;
- (9) Any transmission of information or data by a covered article to a country outside of the U.S.; and Any transmission of information or data by a covered article to a country outside of the U.S., and;
- (10) Any other information that would factor into an assessment of supply chain risk, including any impact to agency mission critical functions, and other information as the FASC deems appropriate.

¹⁵ Interim Final Rule of the Federal Acquisition Security Council.
<https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act#sectno-reference-201.301>. 1SEP2020.

Attachment 5: Hypothetical Examples

The framework and recommendations are demonstrated below using hypothetical examples integrated in the development of a weapon system. The narratives abbreviate what would be a comprehensive development and deployment timeline, highlighting points where OTS HW is involved. Note that the examples are related, but can be reviewed as completely independent; there is repetition amongst the narratives and footnotes.

Example 1: Low Assurance OTS HW

Development has started on a weapon control system; the concept review included operations that require a user console with input and display. The concept development team identified the use of OTS HW as an implementation risk due to supply chain threats¹⁶.

The development team defines requirements related to internal system interfaces with OTS HW: 1) OTS HW shall not have access to system state such that an HWCi 'knows' when the weapon system is ready to fire (Recommendation #16) and 2) system and subsystem interfaces with OTS HW shall satisfy the principles of least functionality and least privilege. Validation of these requirements will be detailed in the MTEPP, which will include independent assessment (similar to Recommendation #28).

The development team conducts a cyber table top during preliminary design after HWCIs have been identified (Recommendation #18). This assessment included a criticality analysis of HWCIs. A mouse input device with USB interface was identified as an HWCi with a criticality Impact Level of III (component failure would cause partial / acceptable mission degradation). A make/buy trade study concludes that a commercial product is the only option (Recommendation #15). The previously mentioned system security requirements serve as countermeasures to supply chain threats related to commercial mice, so the development team identifies the mouse HWCi as a low assurance, LoA 1, HWCi (Recommendation #19).

The mouse HWCi C2 specification does not require much in the way of definition. The development team passively identifies vendors and distributors of COTS mice during the survey phase of OTS HW selection (Recommendation #4). A blind buy is used to purchase the mice (Recommendation #7). Note: assurance efforts in this example were allocated to the system, not the HWCi.

¹⁶ The team identifies risks during implementation tradeoffs and a review of lessons learned from recent development efforts.

Example 2: High Assurance OTS HW

Development has started on a weapon control system; the concept review described operations that require a keyboard, video, and mouse extender (KVM extender which we will refer to as 'KVM' hereafter). The concept development team identified the use of OTS HW as an implementation risk due to supply chain threats¹⁷.

The development team defines requirements related to internal system interfaces with OTS HW: 1) OTS HW shall not have access to system state such that an HWCi 'knows' when the weapon system is ready to fire (Recommendation #16) and 2) system and subsystem interfaces with OTS HW shall satisfy the principles of least functionality and least privilege. Validation of these requirements will be detailed in the MTEPP, which will include independent assessment (similar to Recommendation #28).

The development team conducts a cyber table top during preliminary design after HWCIs have been identified (Recommendation #18). This assessment included a criticality analysis of HWCIs. A KVM with USB, HDMI, and Ethernet interfaces was identified as an HWCi with a criticality Impact Level of I (component failure would result in total mission failure). A make/buy trade study favors a commercial product (Recommendation #15). The previously mentioned system security requirements are only partially implementable; system state necessarily traverses the KVM in plaintext, but least functionality can be satisfied on the USB interfaces. The system host will use a secure parser to satisfy least privilege and least functionality serving as a countermeasure to whole classes of threats inherent to USB interfaces¹⁸. Given the high criticality of the KVM (IL I), the Navy JFAC lab assesses that the KVM is a high assurance, LoA 2, HWCi (Recommendation #19). The development team makes the decision to select and qualify two sources (Recommendation #29) and to impose a 20-minute MTTR requirement for the replacement of a failed KVM on the system.

The SSE and an assurance lab generate a threat tree on the HWCi. The NIAP PP mitigates numerous threats, but attacks on firmware integrity are not mitigated (Recommendations #20 and #21). The KVM C2 specification includes a flow down RMF requirement that the selected products (two sources) be on the NIAP PCL and adds a requirement that controls are in place to protect the integrity of firmware.

Modification is not anticipated as there are a variety of OTS KVM products on the PCL. The development team passively identifies vendors and distributors of COTS KVMs (consulting with the JFAC) during the survey phase of OTS HW selection (Recommendation #4 and #24). Two devices are qualified, which included independent assessments concluding that firmware is adequately immutable (Recommendation #27

¹⁷ The team identifies risks during implementation tradeoffs and a review of lessons learned from recent development efforts.

¹⁸ E. Austin et al. "Toward High-Assurance Interface Protocols For Department Of Defense Applications." <https://apps.dtic.mil/dtic/tr/fulltext/u2/1078548.pdf>. 2019.

and #28). A blind buy is used to purchase the devices (Recommendation #7). Acceptance testing validates the firmware configuration for all assets (Recommendation #30). TTP will leverage tamper protection technology to package spares (Recommendation #31) and an assurance laboratory will conduct failure analyses on returned assets (Recommendation #32).

Example 3: High Assurance Modified Commercial HW

Development has started on a weapon control system; the concept review described operations that require a Versa Module European (VME) processor card. The concept development team identified the use of OTS HW as an implementation risk due to supply chain threats¹⁹.

The development team defines requirements related to internal system interfaces with OTS HW: 1) OTS HW shall not have access to system state such that an HWCI 'knows' when the weapon system is ready to fire (Recommendation #16) and 2) system and subsystem interfaces with OTS HW shall satisfy the principles of least functionality and least privilege. Validation of these requirements will be detailed in the MTEPP, which will include independent assessment (similar to Recommendation #28).

The development team conducts a cyber table top during preliminary design after HWCIs have been identified (Recommendation #18). This assessment included a criticality analysis of HWCIs. The VME card is identified as an HWCI with a criticality Impact Level of I (component failure would result in total mission failure). A make/buy trade study concludes that no OTS products meet interim requirements, but modification to an existing device is feasible (Recommendation #15). The previously mentioned system security requirements are not implementable; mitigating assurance controls will be necessary. The development team proposes adding a WeaselBoard VME card, which provides sensing and logging capability to give indicators of compromise on the VME bus (Recommendation #17). Given the high criticality of the VME card (IL I), the Navy JFAC lab assesses that the VME card is a high assurance, LoA 3, HWCI (Recommendation #19). Qualifying two sources is untenable.

The SSE and an assurance lab generate a threat tree on the HWCI. This complex CI has numerous mitigatable threats, which will require design disclosure for validation.

A process is followed for modified commercial products. The development team actively engages vendors during the survey phase of OTS HW selection, seeking to minimize exposure of program and system information, while documenting said exposure (Recommendations #5 and #6). The JFAC and DIA are engaged to select a vendor (Recommendations #24 and #25). The contract with the vendor for qualification assets

¹⁹ The team identifies risks during implementation tradeoffs and a review of lessons learned from recent development efforts.

includes clauses for delivering vulnerability notification, SW and HW bills of materials, and firmware source code (Recommendations #11 and #22).

The JFAC LoA 3 assessment labs conduct assessments of design artifacts for supply chain risk, exploitability of firmware, and verification of security features (Recommendation #27 and #28). The vendor is able to mitigate some findings via minor design changes; remaining findings are addressed via acceptance testing and TTP during operations.

A blind buy is used to purchase the devices (Recommendation #7). Acceptance testing validates the firmware configuration for all assets (Recommendation #30). TTP will leverage tamper protection technology to package spares (Recommendation #31) and an assurance laboratory will conduct failure analyses on returned assets (Recommendation #32).

DRAFT

OFF-THE-SHELF HARDWARE ASSURANCE GLOSSARY

DRAFT

We borrow some definitions from collaborators at the National Security Agency (NSA) supporting the Joint Federated Assurance Center (JFAC) in order to drive towards commonality with national assurance efforts. *Italicized text represents JFAC language.* Note that the definitions below use the JFAC terms as a baseline, which are not all included in the OTS HW framework.

3rd Party IP (3PIP) – *3PIP is a functional unit designed by a different organization than the principle design team. Typically, 3PIP is a pre-existing design, offered for sale by a commercial organization.*

Application Design – *The collection of schematics and other design artifacts like source code developed to generate applications or other programmable configurations that run atop OTS hardware platforms.*

Application Domain – *This is the area of technology of the system itself, or a directly associated area of technology. For instance, the system technology domain of a radar system implemented using FPGAs would be "radar" or "electronic warfare."*

Application Specific Integrated Circuit (ASIC) – *A microelectronic component that is designed for a specific limited purpose. For example, OTS HW devices commonly contain ASICs to manage functions for individual communication protocols like USB and Ethernet. An ASIC cannot be repurposed/reprogrammed to perform another function unlike microcontrollers or CPUs, which can arbitrarily be programmed for any number of purposes.*

Configuration File – *Specific to FPGAs. The set of all data produced by the application design team and loaded in to an FPGA to personalize it. Referred to by some designers as a "bitstream" the configuration file includes that information, as well as additional configuration settings and firmware, which some designers may not refer to in the term "bitstream."*

Field Programmable Gate Array (FPGA) – *For the purposes of this document, we define FPGA to include the full range of devices containing substantial reprogrammable digital logic. This includes devices marketed as FPGAs, CPLDs, SoC FPGAs, as well as devices marketed as SoCs and containing reprogrammable digital logic.*

Latent Vulnerability – *There is not an agreed upon, canonical, definition of latent vulnerabilities. Latent vulnerabilities may include exploitable defects, which in nature are escapes from quality control. This can also include legitimate features that are exploitable to achieve an adversary's objectives (e.g., undocumented features, test modes, rich features possessed by a commercial device that are used by certain customers, but not in the DoD POR system, etc.).*

Level of Assurance (LoA) – *A Level of Assurance is an established guideline that allows mitigations to be selected appropriate to a specific circumstance, without the need for*

system-by-system custom evaluation. The JFAC uses Levels of Assurance LoA 1/2/3 to prescribe mitigations based on applicable threat categories.

OTS HW – OTS HW or Off-the-Shelf Hardware describes commercially available hardware that includes ICT (information communications technology), TMDE (test, measurement, and diagnostic equipment), and other commercial hardware that has some degree of computing electronics therein. Examples include commercial power supplies, power conditioners, industrial control systems, portable computing devices, enterprise computing devices (e.g. servers/workstations), network appliances, storage devices (e.g., solid state drives or network attached storage), commercial bus/backplane computing, GPS receivers, printers, LCD displays, mice, keyboards, oscilloscopes, environmental monitoring equipment, test sets, etc.

Platform – *A platform refers to a specific device/product type or family of devices/products from a vendor. For example, Intel's Stratix 10 series of chips is an FPGA Platform and Cisco's Nexus 5000 series of network devices is an Ethernet Switch Platform.*

Platform design – *The platform design is the set of design information that specifies the platform, including printed circuit boards, bills of materials, physical layouts of microelectronic devices, code, etc.*

Soft IP – *Soft IP is a hardware design captured in HDL, intended to be integrated into a complete hardware design through a synthesis process. Soft IP can be distributed in a number of ways, as functional HDL or a netlist specified in HDL, encrypted or unencrypted.*

System – *A collection of related hardware and data comprising a final product or sub-component of a final product (i.e., what acquisition programs of record engineer and deliver). We seek to provide assurance to systems. A system may be a complete weapons system, or a sub-component of that system. When we discuss assurance, we are trying to protect the system from threats related to its use of FPGA technology.*

System design – *System design is the set of information that defines the manufacturing, behavior and programming of a system. It may include subsystem designs, board designs, firmware, software, FPGA configuration files, etc.*

Target – *A target refers to a specific deployed instance of a given system, or a specific set of systems with a common design and function.*

Targetability – *The degree to which an attack may have an effect that only shows up in circumstances the adversary chooses. An attack that is poorly targetable would be more likely to be discovered accidentally, have unintended consequences, or be found in standard testing. Captures the usefulness and reliability of an attack.*

Threat Category – *A threat category refers to a part of the supply chain with a specific attack surface and set of common vulnerabilities, against which many specific attacks*

may be possible. We use this term to refer to a wide array of specific attacks an adversary might carry out against a specific region of the supply chain.

Utility – The utility of an attack is the degree to which an effect has value to an adversarial operation. Higher utility effects may subvert a system or provide major denial of service effects. Lower utility attacks might degrade a capability to a limited extent.

DRAFT