Defense Trade Advisory Group (DTAG)

Cyber Working Group White Paper

October 29, 2015

DTAG Working Group Members

Co-chairs: Rebecca Conover & Larry Fink

Marjorie Alquist
Fred Czarske
Julia Court Ryan
Susan Willard
Michelle Avallone
Kelly Hochstetler
William Schneider
Larry Ward

Table of Contents

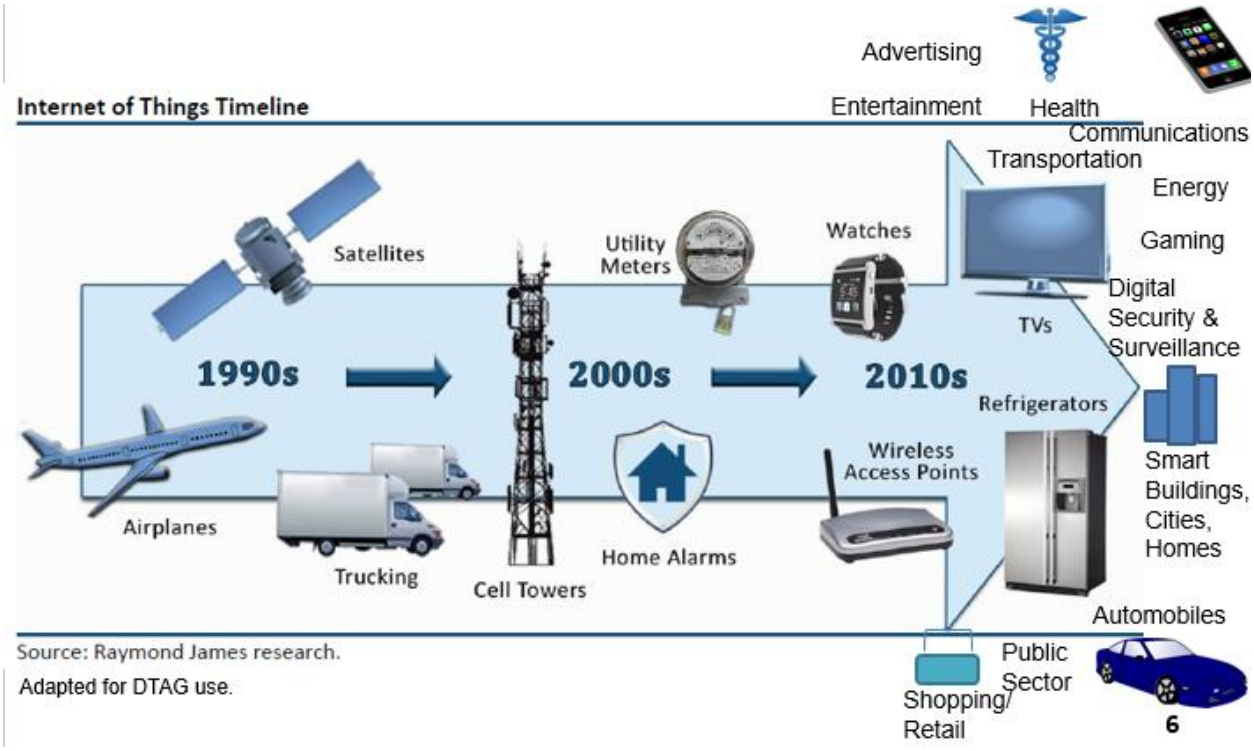
DTAG Task:

Define and categorize “cyber products” in an export control context and determine:

- Which cyber products, if any, should be included on the U.S. Munitions List
- The types of controls appropriate for each cyber category
- The potential impact on cyber products, including but not limited to Big Data Analytics
- How the recommendation differs from how cyber products are controlled today and why

Background/Definition

Cyber technology does not fit easily into discrete technology categories or taxonomies and is broadly used to describe activities involving or related to network connectivity, computer software and hardware, and any other product that uses computational technology. The term is broadly used in many contexts with another word as an adjective indicating that computers are involved: cyber space, cyber warfare, cyber security, cyber bullying…even cyber Monday. The Working Group observed that the term cyber may involve anything in what is now known as the “Internet if Things” – a term that characterizes items connected with electronics, software, sensors, etc. creating a network of connectivity. As depicted in the diagram below, the growth of cyber technology has exploded over the past 20 years and is now present in many commercial products offered across the global economy and offered to consumers with little or no restriction.



Methodology

The DTAG examined the historical regulatory controls and trends in computing and cyber products and researched proposed and existing cybersecurity rulings and industry comments. The team then explored existing regulations and jurisdiction rulings affecting cyber and Big Data Analytics and examined the global availability of the related technology. Upon completion of that research, the team defined the three general cyber product categories with assistance from in-house cyber experts from industry. Finally, the DTAG studied cyber and data analytics product development and global availability of the related technology.

For the purposes of the DTAG Tasking, the Working Group identified three primary cyber technology categories to examine: 1) Cyber Security, 2) Data Collection and 3) Big Data Analytics. To arrive at these three broad categories, the Working Group researched and enumerated all the areas of cyber relevant to the task and placed each one into a broader category. The three that were selected for the Tasking broadly covered every unique cyber item or technology that the DTAG identified.

In order to ensure focus, the Working Group identified three areas related to cyber that were sufficiently addressed in the existing regulations or the subject of separate debate outside of the DTAG. The three areas considered "out of scope" of this Tasking are: 1) Encryption, 2) Cloud Computing Controls (Harmonization Rule & Prior DTAG tasking[1]), 3) Cryptography USML Category**.**

Cybersecurity

As with the definition of "cyber technology", there is no single definition of "cybersecurity". The National Institute of Standards and Technology ("NIST") defines cybersecurity as "[t]he ability to protect or defend the use of cyberspace from cyber attacks."[2] There are numerous cybersecurity products currently available commercially. In addition, there is a considerable amount of cybersecurity research and development taking place within industry and academia to better detect, monitor, analyze and thwart cyber threats, thereby improving cyber defenses.

The DTAG reviewed currently available and emerging cybersecurity technologies and parsed these technologies into broad categories based upon their functional capabilities (e.g., access controls, threat detection and monitoring, and protective countermeasures). These capabilities are delivered through multiple channels, including hardware, software, firmware, services, or a combination thereof.

After reviewing a range of cybersecurity products, their functional capabilities and delivery methods, the DTAG concluded that the performance capabilities found in cybersecurity technologies are inherently "dual use" technologies. Although customization of available or emerging cybersecurity products to meet military or defense needs may warrant control under the ITAR, the essential underlying capabilities and delivery methods do not. Furthermore, the DTAG concluded that there is little to no

[1] For the DTAG report on cloud computing, see http://pmddtc.state.gov/DTAG/index.html.
[2] *Glossary of Key Information Security Terms*, NISTIR 7298 Revision 2, R. Kessel (ed.)., available at http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

distinction between offensive and defensive uses of cybersecurity products: most of the performance capabilities of cybersecurity products can be used for both good and ill. For example, the capabilities and methods used to test a system's vulnerability to cyber threats can be used offensively and defensively. Vulnerability testing can be used to search for a system's weakness and exploit it. At the same time, vulnerability testing can be used by a company to search its own system in order to assess and address vulnerabilities, thereby improving the system's cyber defenses on the whole. The inability to distinguish between a particular cybersecurity capability as offensive or defensive was characteristic of all the cybersecurity products reviewed by the DTAG.

Data Collection

Data Collection is the second general category of "cyber" items identified by the DTAG. While this area is very broad, the DTAG deemed it an important one to include as this category directly relates to the other primary categories and has become increasingly important as an enabler of cyber security and data analytics. Through the DTAG Working Group's research, the team identified that the existing export controls on data collection are appropriately low barriers. Generally the export control on data collection matches the jurisdiction and classification of the data being collected. In many cases, the more significant controls on data collection are applicable when personal information is collected and privacy controls are invoked. The DTAG does not recommend any change to the export controls on data collection.

Big Data Analytics

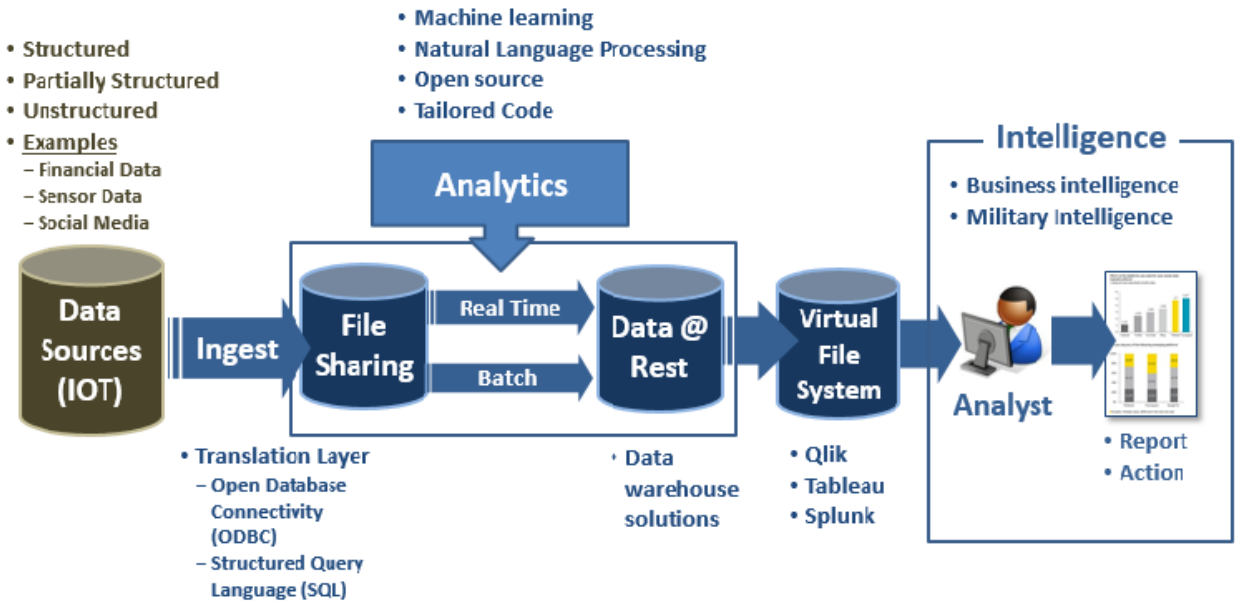
The third primary area of "cyber" identified by the DTAG is Big Data Analytics. Based on discussions with technical experts and a survey of public domain information, the group identified three primary features of Big Data Analytics:

- Data Ingestion. Large amounts of data are ingested for further analysis. Some data may be in a usable format for further analysis while other data is partially structured or unstructured, requiring further refinement before it can be analyzed.
- Data Analytics. Through use of various filtering and analytic techniques, the data is sorted and categorized resulting in structured and analyzed output for the end user.
- End user analysis. Based on the output, analyst reviews the data and produces a report or initiates actions.

Similar to cyber security, the technical building blocks for analytics products are not differentiated by commercial versus non-commercial uses. With the exception of some specific tailored analytic algorthims, the identical or similar software and algorithms used for military intelligence purposes are also used for business intelligence. The primary points of differentiation for are in the types of data ingested and the back end human analysis of the output.

Below is a flow chart showing the high level flow of information and items utilized for data analytics. The DTAG noted that the unique military or intelligence customization for analytics items occurs in the last phase of the process, and therefore, determined that the most appropriate control for analytics items is at the final stage of the process or when special tailored algorithms are developed. Controlling the more

generic analytics items is counter to export control reform and will also limit the ability of businesses to utilize data analytics for valuable commercial purposes.



Themes & Findings

The Working Group reviewed the research and identified the general themes and findings. These themes and findings represent fact based observations based on the group's research and were the basis for final recommendations.

- Cyber technology is becoming omnipresent in virtually all human endeavors and activities worldwide and heading to a future of ubiquitous computing. As previously noted, cyber technology is present in many consumer products and available across the global economy.
- Cyber products, including Big Data Analytics, are designed and available throughout the world.
- There is little or no technical distinction between offensive and defensive cyber capabilities. Developers of cyber security products typically use hacking and malware technology to test, improve and refine their products. Technology used to mount an attack against a network, for example, is identical to or based upon technology used to protect a network.
- Cyber security products for commercial and military purposes are developed using fundamentally the same computing products and technologies that are globally developed and available. For this reason, broad technical export controls will hinder scientific progress and research and development.
- There is little or no technical difference between Big Data Analytics products used for military intelligence purposes and commercial business purposes. The basic technology building blocks are the same.
- The rapidly evolving nature of cyber technology does not lend itself to controls based on technical parameters associated with performance capabilities.

Moreover, cyber security capabilities are developed, enhanced and tested by utilization of hacking and malware items that may be considered to be defense articles.

DTAG Working Group Recommendations

1. Cyber products currently controlled under the EAR are dual-use and should not be transferred to the USML.

   The Working Group evaluated the many areas of the export regulations that currently address cyber-related technologies, software and items. The Working Group not only observed that the appropriate controls appear to be in place, but also thinks that it is contrary to Export Control Reform to increase controls on existing items. Additionally, the DTAG did not identify any categories of cyber products or technology that warrant additional control.

2. Remove or significantly revise USML Category XI(b)

   USML category XI(b) is overreaching and captures products that are not uniquely military. The DTAG Working Group determined that the necessary controls are captured under other categories such as USML XIII or XVII. Additionally, unique military customization is controlled as a defense service so items not enumerated on the USML will still be controlled through the specific services.

3. Controls on cyber products (including data analytics) should be predominantly end-use or end-user based versus being enumerated on the USML.

   Technology-based ITAR controls for cyber products may be counterproductive to national security due to the collaborative development process imperative for cyber security products. Commercial (and non-commercial) cyber security features are developed, enhanced and tested by using hacking and malware products that could be considered to be defense articles. Restricting the hacking and malware products from export would negatively impact commercial cyber security development. By using end-use or end-user controls, the US government can restrict access to specific parties without jeopardizing the development of critical cyber products.

Summary

In order to stay at the forefront of technical advancement, only a very few cyber products should be controlled under the ITAR. Dual-use and ITAR controlled items both benefit from the advancement of general technical capabilities. The DTAG recommends that the Dept. of State only control cyber products if they are classified or are positively enumerated on the USML.

Appendix 1 - Cyber Category Identification

Cyber Category	Specific Cyber Item
Big Data Analytics	Big Data Analytics Products
Cyber Security	Intrusion Software - for detection & intrusion
Cyber Security	Access control (Defensive cybersecurity products/technology)
Cyber Security	Offensive cybersecurity products/technology
Cyber Security	Detection evasion products from anti-malware
Cyber Security	Access Control - Digital Rights Management software
Cyber Security	Hypervisors, debuggers, or Software Reverse Engineering tools
Cyber Security	"Network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices"
Cyber Security	Surveillance items
Cyber Security	Vulnerability research
Cyber Security	Cybersecurity - securing data, systems, codes with encryption (e.g. in a cloud)
Cyber Security	Access Control - preventing changes to code (Kevlar)
Big Data Analytics	Big data mining - how to mine & analyze
Cyber Security	vulnerability testing - offensive/defensive tools
Cyber Security	Access Management
Cyber Security	VPN - Identity Management
Cyber Security	Network, Information, Application Security
Big Data Analytics	Disaster Recovery/business continuity planning
Cyber Security	Antivirus
Cyber Security	Spyware
Cyber Security	cyber intrusion
Data Collection	cyber event monitoring
Cyber Security/Data Collection	cyber incident / reportable cyber incident
Data Collection	Social Media Monitoring
Cyber Security	TEMPEST

Appendix 2 - SELECTED GLOSSARY OF KEY INFORMATION SECURITY TERMS

Source: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

---

Advanced Persistent Threats (APT) – An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.

Anomaly-Based Detection – The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.

Anti-jam – Countermeasures ensuring that transmitted information can be received despite deliberate jamming attempts.

Anti-spoof – Countermeasures taken to prevent the unauthorized use of legitimate Identification & Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker.

Antispyware Software – A program that specializes in detecting both malware and non-malware forms of spyware.

Antivirus Software – A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

Approved Security Function – A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either a) specified in an Approved Standard; b) adopted in an Approved Standard and specified either in an appendix of the Approved Standard or in a document referenced by the Approved Standard; or c) specified in the list of Approved security functions.

Assurance – Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.

In the context of OMB M-04-04 and this document, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Automated Security Monitoring – Use of automated procedures to ensure security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the information system.

Backdoor – An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.

Baseline Security – The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection.

Biometric System – An automated system capable of: 1) capturing a biometric sample from an end user; 2) extracting biometric data from that sample; 3) comparing the extracted biometric data with data contained in one or more references; 4) deciding how well they match; and 5) indicating whether or not an identification or verification of identity has been achieved.

Boundary Protection – Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Brute Force Password Attack – A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords.

Buffer Overflow – A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.

Certified TEMPEST Technical Authority (CTTA) – An experienced, technically qualified U.S. government employee who has met established certification requirements in accordance with CNSS-approved criteria and has been appointed by a U.S. government department or agency to fulfill CTTA responsibilities.

Chief Information Officer (CIO) – Agency official responsible for: 1) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; 2) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and 3) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Cloud Computing – A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent

resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud). ***Note***: Both the user's data and essential security services may reside in and be managed within the network cloud.

Commercial COMSEC Evaluation Program (CCEP) – Relationship between NSA and industry in which NSA provides the COMSEC expertise (i.e., standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product. Products developed under the CCEP may include modules, subsystems, equipment, systems, and ancillary devices.

Common Vulnerabilities and Exposures (CVE) – A dictionary of common names for publicly known information system vulnerabilities.

Communications Security – (COMSEC) -- A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material.

Community of Interest (COI) – A collaborative group of users who exchange information in pursuit of their shared goals, interests, missions, or business processes, and who therefore must have a shared vocabulary for the information they exchange. The group exchanges information within and between systems to include security domains.

Computer Network Attack (CNA) – Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defense (CND) – Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.

Computer Network Exploitation (CNE) – Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks.

Computer Network Operations – (CNO) Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

Controlled Unclassified Information (CUI) – A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces "Sensitive But Unclassified" (SBU).

Data Encryption Algorithm (DEA) – The DEA cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA).

Data Security – Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Defense-in-Depth – Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.

Denial of Service (DoS) – The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Exploit Code – A program that allows attackers to automatically break into a system.

Federal Information Security Management Act (FISMA) – A statute (Title III, P.L. 107-347) that requires agencies to assess risk to information systems and provide information security protections commensurate with the risk. FISMA also requires that agencies integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to OMB.

Global Information Grid (GIG) – The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

Global Information Infrastructure – (GII) Worldwide interconnections of the information systems of all countries, international and multinational organizations, and international commercial communications.

Honeypot – A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators.

IA Architecture – A description of the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

Inadvertent Disclosure – Type of incident involving accidental exposure of information to an individual not authorized access.

Independent Verification & Validation (IV&V) – A comprehensive review, analysis, and testing (software and/or hardware) performed by an objective third party to confirm (i.e., verify) that the requirements are correctly defined, and to confirm (i.e., validate) that the system correctly implements the required functionality and security requirements.

Information Operations (IO) – The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making process, information, and information systems while protecting our own.

Information Security –– Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— 1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; 2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and 3) availability, which means ensuring timely and reliable access to and use of information.

Inside(r) Threat – An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.

Intrusion Detection Systems (IDS) – Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)

IT-Related Risk – The net mission/business impact considering 1) the likelihood that a particular threat source will exploit, or trigger, a particular information system vulnerability, and 2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to: ω Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information; ω Non-malicious errors and omissions; ω IT disruptions due to natural or man-made disasters; or ω Failure to exercise due care and diligence in the implementation and operation of the IT.

Malware – A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Multilevel Security (MLS) – Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.

National Information Assurance Partnership (NIAP) – A U.S. government initiative established to promote the use of evaluated information systems products and champion the development and use of national and international standards for information technology security. NIAP was originally established as a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under P.L. 100-235 (Computer Security Act of 1987). NIST officially withdrew from the partnership in 2007 but NSA continues to manage and operate the program. The key operational component of NIAP is the Common Criteria Evaluation and Validation Scheme (CCEVS) which is the only U.S. government-sponsored and endorsed program for conducting internationally recognized security evaluations of commercial off-the-shelf (COTS) Information Assurance (IA) and IA-enabled information technology products. NIAP employs the CCEVS to provide government oversight or "validation" to U.S. CC evaluations to ensure correct conformance to the International Common Criteria for IT Security Evaluation (ISO/IEC 15408).

NSA-Approved Cryptography – Cryptography that consists of: (i) an approved algorithm; (ii) an implementation that has been approved for the protection of classified information in a particular environment; and (iii) a supporting key management infrastructure.

Operations Security (OPSEC) – Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Outside(r) Threat – An unauthorized entity outside the security domain that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Packet Sniffer – Software that observes and records network traffic.

Penetration Testing –Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Proprietary Information (PROPIN) – Material and information relating to or associated with a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that has been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the government or to the public without restriction from another source.

Resilience – The ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.

Sanitization – PA general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.

Security Categorization –The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.

Spillage – Security incident that results in the transfer of classified or CUI information onto an information system not accredited (i.e., authorized) for the appropriate security level.

TEMPEST – A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

Trustworthy System – Computer hardware, software and procedures that— 1) are reasonably secure from intrusion and misuse; 2) provide a reasonable level of availability, reliability, and correct operation; 3) are reasonably suited to performing their intended functions; and 4) adhere to generally accepted security procedures.

Virtual Machine (VM) – Software that allows a single host to run one or more guest operating systems.