UNCLASSIFIED

DSS Industrial Security Asset Identification Guide

Version 2.1
October 2018

UNCLASSIFIED

CONTENTS

1 INTRODUCTION

This publication, the Industrial Security Asset Identification Guide (AIG) was produced by the Defense Security Service with support from U.S. Government interagency and private industry partners.

The need to better align Government and Industry perspectives on the breadth and depth of assets under the industrial security umbrella was identified during the DSS in Transition initiative.

As the Public-Private Partnership strengthens to enhance protection of our national security and industrial security programs, a common understanding of asset identification will improve standardization, reporting, and ultimately the provision of more timely and targeted threat information to industry partners.

PURPOSE

The DSS Industrial Security Asset Identification Guide (AIG) is intended to provide a coherent conceptual framework and an operational vocabulary to align Government and Industry identification of assets related to DoD national security programs.

APPROACH

The AIG is a "living" document that is reviewed periodically to ensure accuracy, relevance, and currency against the ever-changing counterintelligence threat. Recommended changes and updates are accepted continually and will be considered during the review process. Updated editions will be submitted and approved by a public-private working group focused on industrial security.

OBJECTIVES

The AIG supports three core objectives related to enhancing industrial security which will be realized at different points throughout the transition to a new industrial security methodology:

- Cataloging industrial security assets, permitting deeper security reviews
- Standardizing and elevating FSO capabilities nationally
- Permitting delivery of more tailored, applicable threat information to industry

POTENTIAL ASSETS

WHERE TO DRAW THE LINE?

You wouldn't have hired them if they weren't important, right? The argument can be made that every employee, as well as every tool, supplier, and nugget of data is an asset critical to a program's uncompromised delivery. True though that is, security professionals lack the resources to truly protect everything. Some determination must be made to prioritize all the items that need to be protected.

This Asset Identification Guide seeks to help security professionals with an important question:

"What could be an asset?"

The items identified by using this guide are just that: Potential assets.

From there, a determination must be made to prioritize those items which are most likely to lead to compromise of programs.

How security professionals decide to focus their efforts once potential assets are identified is not covered in this guide. However, it is recommended that professionals use a logical model which includes both Likelihood and Consequence of loss or compromise. When identifying assets, it's important to focus on a manageable selection of items to protect. Layering this subjective information with available threat data should provide focus for prioritization.

CRITICAL THINKING

Security professionals will need to think critically about their programs, technologies, and facilities when using this Asset Identification Guide. Working with program managers, scientists, engineers, marketing, finance, and other employees around the firm will help identify what subject matter experts in your firm would consider exploitable pieces of information to compromise our critical programs.

LAYERING

One construct to consider is whether a potential asset sits across multiple categories. This layered approach might be used to assess likelihood and consequence from multiple angles, or to compare the criticality of potential assets.

USING THIS GUIDE

The AIG is designed to help security professionals better understand their organizations and programs in the context of critical assets. It provides seven primary asset categories, and further breaks them down to an increasing degree of specificity. This AIG is not all encompassing; local security professionals may – and are encouraged to - recognize assets they believe to be critical to our national and economic security and superiority.

This guide breaks assets down into three tiers. Security professionals are encouraged to identify assets at the lowest level possible, as it will help with the level of threat information which can eventually be provided in return.

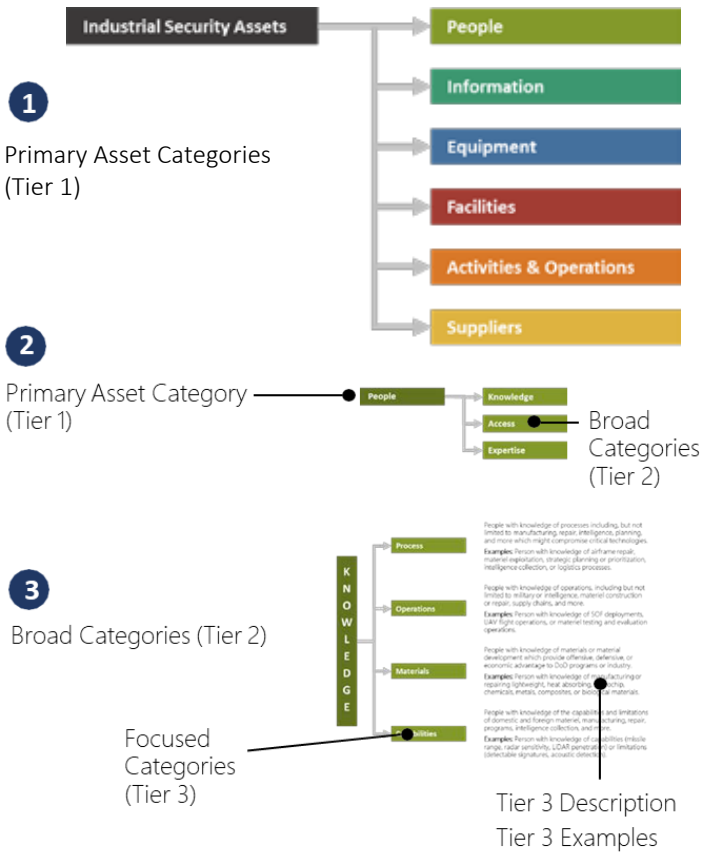
These three tiers are:

- Tier 1 – Primary Categories
- Tier 2 – Broad Categories
- Tier 3 – Focused Categories

Illustrative examples are provided for specific categories

.

The AIG helps security experts explore each Tier 1 asset type by providing a guide into each category to assist with identifying and cataloging assets.



PEOPLE

People mark one of the single most critical assets to national security. The knowledge, access, and expertise resident in our cleared workforce around the globe is both our greatest strength and our largest vulnerability. The curiosity, tenacity, and innovative nature of our people is what drives the Defense Industrial Base. No matter how hard we train, there will always be ways in which our people can intentionally or, more frequently, unintentionally jeopardize our national security information.

When categorizing people, this guide focuses on cataloging attributes related to where our adversaries might be interested in focusing intelligence efforts.

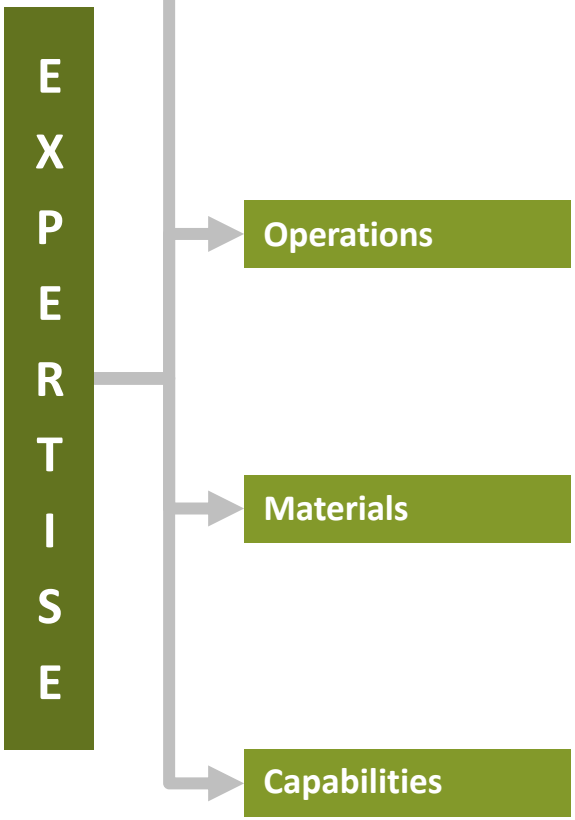
Critically, it's recognized that while the entire cleared workforce is crucial to success, industry's ability to focus protective measures based on tailored threat information requires a clear look at assets up front. As such, every member of the workforce may not fit into a category. Evolutions in priorities and threats may change this categorization over time.

PEOPLE ASSET DEFINITION

People are considered assets based on the knowledge they possess, the access they maintain, the expertise they provide, or the influence they possess.

- Expertise – Knowledge or experience in a given area
- Access – Ability to access spaces, programs, and data
- Influence – Ability to shape or control

5



People with knowledge or experience with processes such as manufacturing, repair, intelligence, planning, and more which might compromise critical programs.

Examples: Person with knowledge of airframe repair, materiel exploitation, strategic planning or prioritization, intelligence collection, or logistics processes.

People with knowledge or experience of operations such as military or intelligence, materiel construction or repair, supply chains, and more.

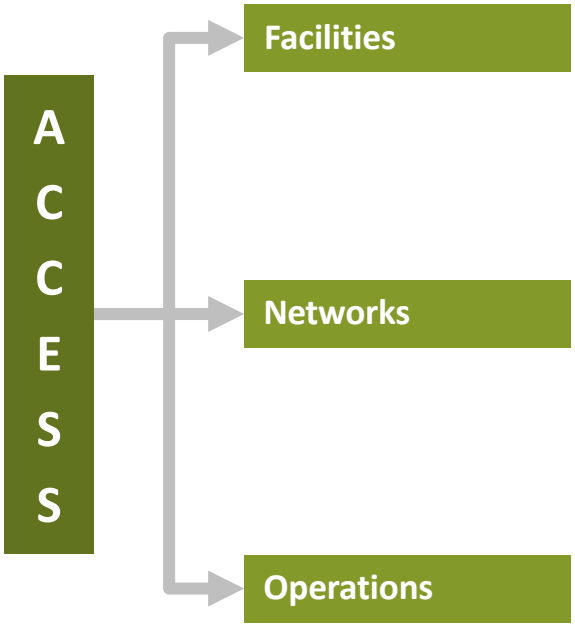
Examples: Person with knowledge of SOF deployments, UAV flight operations, or materiel testing and evaluation operations.

People with knowledge or experience of materials or material development which provide offensive, defensive, or economic advantage.

Examples: Person with knowledge of manufacturing or repairing lightweight, heat absorbing, microchip, chemicals, metals, composites, or biological materials.

People with knowledge or expertise with the capabilities and limitations of materiel, manufacturing, repair, programs, intelligence collection, and more.

Examples: Person with knowledge of capabilities (missile range, radar sensitivity, LiDAR penetration) or limitations (detectable signatures, acoustic detection).



People with access to facilities or infrastructure with materiel, components, information, data, networks, plans, strategies, or more.

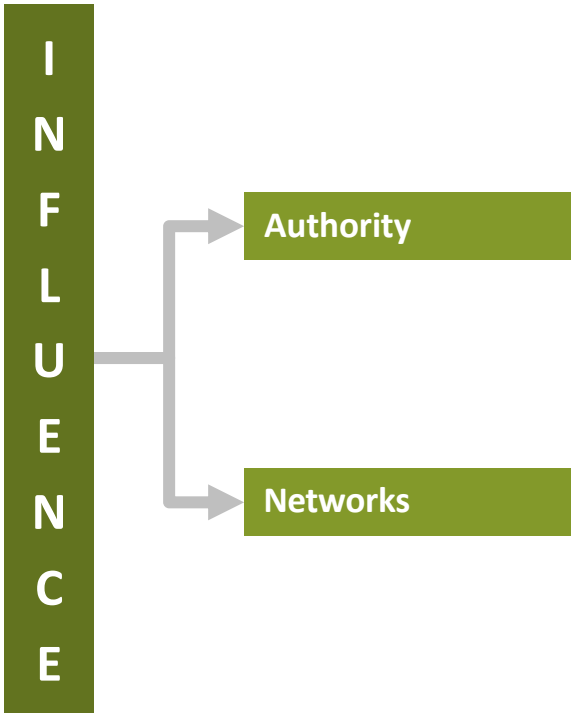
Examples: Person with access to server rooms, assembly areas, mechanical spaces, SCIFs, lockers, RDT&E sites, or storage areas.

People with access to networks with Industry proprietary, Government, or other data, information, or intelligence products.

Examples: Person with access to program test data, administrator access to networks, classified networks with technology detail, or networks with proprietary methods.

People with access to activities or operations related to programs, capabilities, or technologies, to include deployments, testing, development, and more.

Examples: Person with access to materiel testing and evaluation operations, aircraft carrier re-fueling, intelligence collection, or military planning operations.



People with authority over individuals or process, possessing the capacity to direct activities of people and/or decision making ability.

Examples: People with authorities related to purchasing, hiring and terminating employees, release and distribution of data, etc.

People with influential, protected, or specialized networks, either internal or external to the organization which might permit access to classified programs.

Examples: People with access to corporate leadership or Government officials, specialized trade groups or subject matter experts, etc.

INFORMATION

Information is both the simplest and most nebulous of the asset categories to define. Identifying information in a manner which enables security professionals to act in a manner unique and separate from the protection of people or equipment.

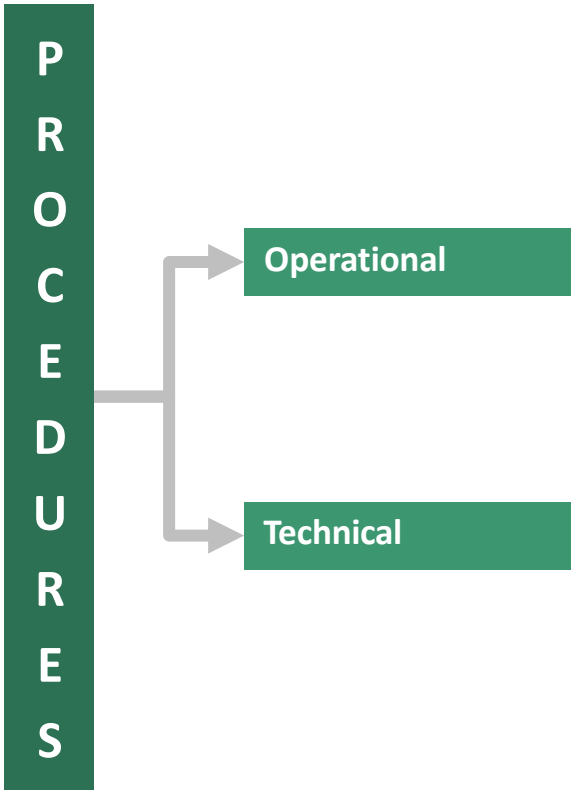
By examining information across four lenses – Procedures, Capabilities, Networks, Data, and Corporate – this guide intends to help security professionals identify different pieces of information which may provide basic or complex insight into programs or technologies.

While all classified information requires security and protection, the focus of this guide are those pieces of information which require more active security controls in light of their ability to detrimentally compromise priority technologies related to industrial security.

INFORMATION ASSET DEFINITION

Information includes the procedures, capabilities, data, and corporate information which enable military and economic superiority.

- Procedures – Processes or steps necessary for a task
- Capability – Information related to a program's capabilities
- Data – The raw or processed data surrounding a program
- Corporate – Proprietary data related to a company's operations

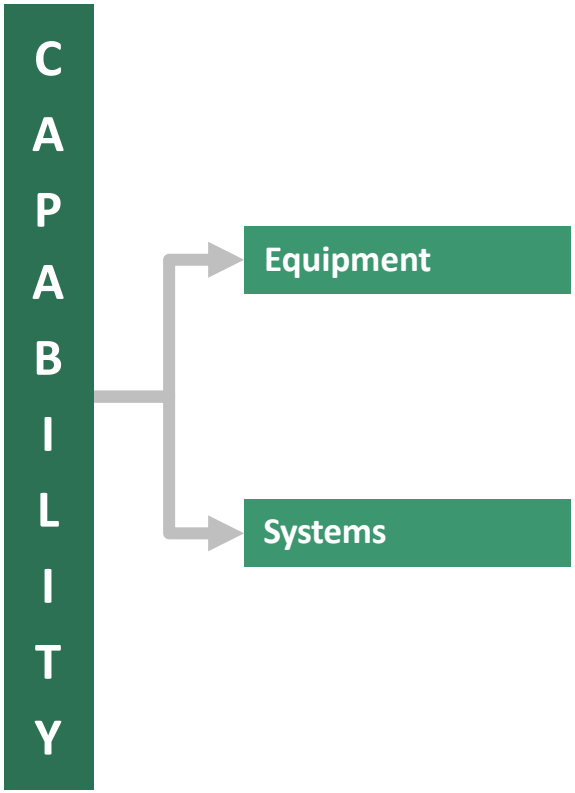


Information which outlines operational procedures, to include the development or execution of military or industrial strategies, plans, or development goals.

Examples: Procedures for developing or executing battle plans, Joint Publications on strategy, or DoD guidance regarding fiscal year planning.

Information which outlines technical procedures, to include field or depot-level repair manuals, material development instructions, or materiel usage guidance.

Examples: Technical Publication for the specific repair procedures on damaged equipment or a manual outlining the maintenance cycles for helicopter engines.

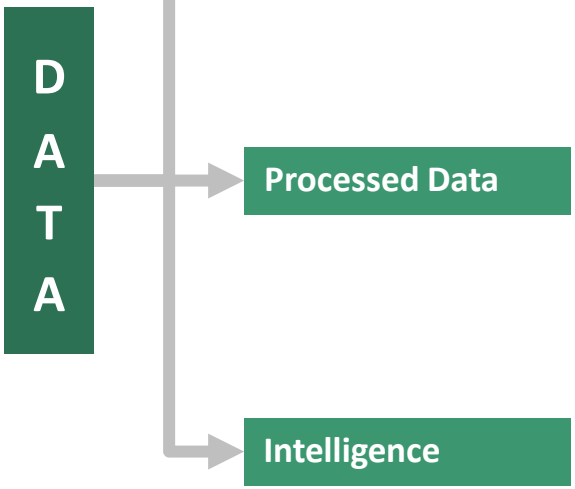


Information on specific equipment capability, vulnerability, or limitations which provide industrial, economic, or military advantage.

Examples: Program test documentation on LiDAR system penetration or acquisition documentation outlining Key Performance Parameters.

Information on systems (system-of-system) capability, vulnerability, or limitations which provide industrial, economic, or military advantage.

Examples: Test results of system effectiveness or acquisition documentation with Key Performance Parameters on DCGS or CEC-like capabilities.



Raw data are the unprocessed inputs from sensors, materiel, or equipment which exist without context, yet could still compromise capability or technology.

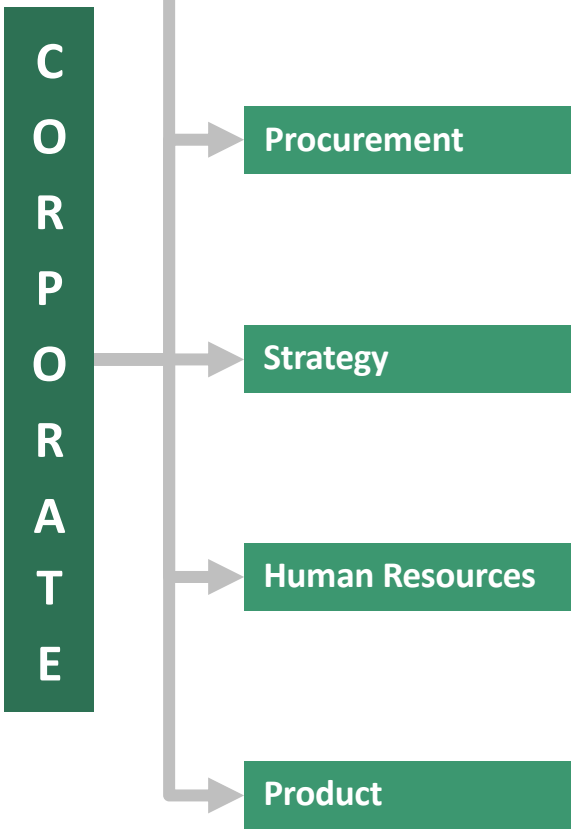
Examples: Temperature readings, test results, single performance score, sensor inputs, raw images, or primary intelligence source reporting.

Processed data includes context for the data which provides additional meaning, having likely been obtained during analysis, vetting, or other means.

Examples: LiDAR penetration readings, processed ISR platform imagery, validated intelligence source reporting, or engine temperature readings by climate.

Intelligence includes products derived from any traditional intelligence collection methods which may be more specific than simply of raw or processed data.

Examples: Signals analysis, adversary troop relocation frequency, foreign surface-to-air missile placement and range, or materiel signatures.



Financial information includes any public or non-public information which might reveal insight into programs.

Examples: Corporate investments, internal R&D spending, divestitures, acquisitions, etc.

Procurement information pertains to the purchasing behavior of a company surrounding a program.

Examples: Laboratory testing equipment, specific raw material sourcing, PPE for Nuclear materials, etc.

Information on strategy pertains to corporate perspective or knowledge of customer requirements.

Examples: Opening a new office, merger & acquisition roadmaps, or business development campaigns.

Human Resources information includes corporate-held data that might be used to compromise an individual.

Examples: Wage garnishments, disciplinary actions, PII, timesheet and project billing information, etc.

Information regarding proprietary, non-Governmental, or COTS products supporting programs.

Examples: Portable mass spectrometer capabilities, rubber compound heat tolerances, etc.

13

EQUIPMENT

Whether designing discrete components or providing support staff to headquarters operations, industry possesses a huge volume and variety of equipment which supports the DoD and USG. This guide examines equipment through three lenses which require active security controls above and beyond compliance: Materiel, Industrial, and Supporting Equipment.

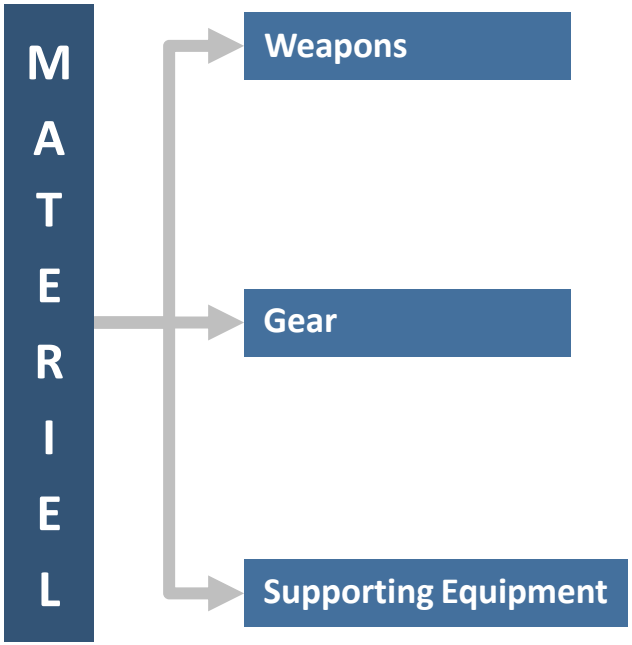
Across these categories, security professionals are encouraged to work with operators, engineers, and others to understand how the compromise of seemingly mundane repair tooling might reveal critical program details.

The challenge under equipment exists most clearly for companies focusing on support services contracts. For these, security professionals are challenged to examine enabling and supporting equipment used in and around the support team which might be compromised and detrimentally impact related technologies.

EQUIPMENT ASSET DEFINITION

Equipment is tangible property (other than land or buildings) determined to be essential for the warfighter, industrial base, or supporting activities.

- Materiel – Equipment related to deployable assets supporting operations
- Industrial – Equipment related to industrial processes
- Supporting – Equipment which supports classified programs
- Networks – Internal and external servers and networks



Weapons or weapon systems either in development or full operational capability physically under the control or cognizance of an organization.

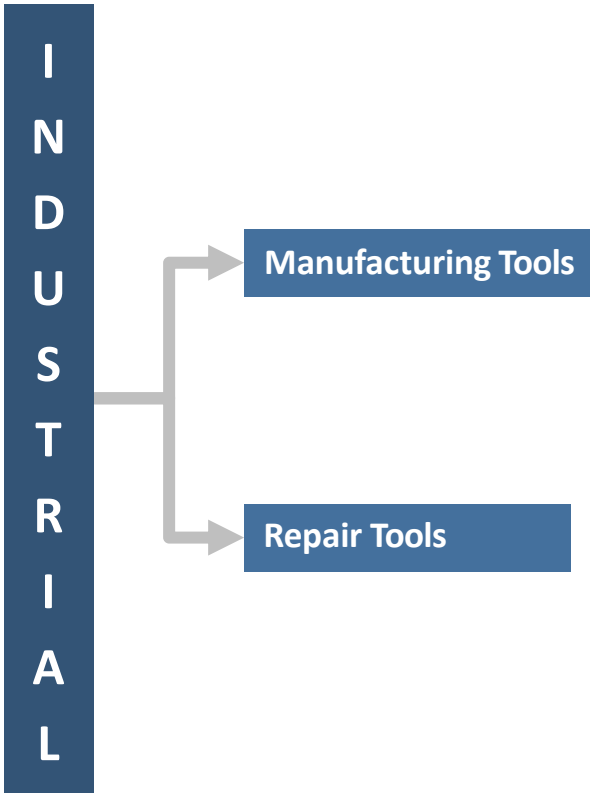
Examples: Test and evaluation vehicles provided for computer adjustment, or missiles and components being manufactured at a facility.

Gear includes the enabling materiel warfighters rely on outside weapons systems, to include optical, navigational, logistical, communications, or sustainment.

Examples: Low-light optical equipment, radios, ballistics vests, prepositioned materiel, navigation equipment, or soldier helmets.

Supporting equipment includes sustainment, protection distribution, or preservation, of both weapons and gear and may in itself give access to compromise programs.

Examples: Handling or packaging which may lend insight into fragility or vulnerability of materiel; refrigeration systems which may reveal performance limitations.

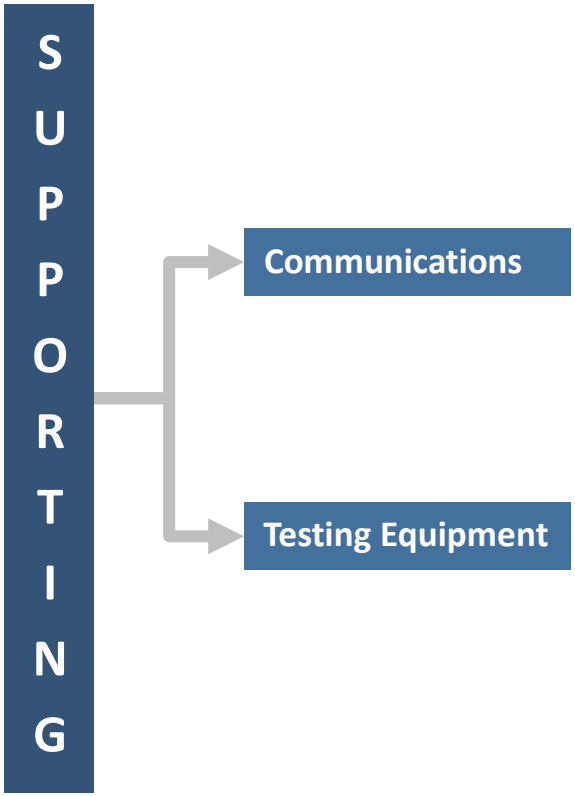


Industrial manufacturing tools are those specially designed or employed pieces of equipment which permit the assembly or manufacture of technologies.

Examples: Specially designed robots in microchip plant; commercial tools modified to serve DoD purposes, or assembly plant automated systems.

Industrial repair tools are those specially designed or employed tools which permit the efficient, rapid, safe, or uncompromised repair of a technology or program.

Examples: Compounds used to secure damaged airframe components or specially designed repair tools for nuclear reactor environments.

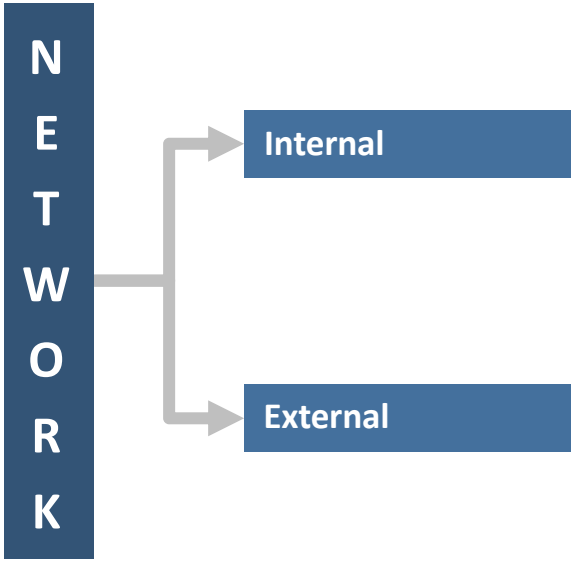


Supporting communications equipment includes phones, servers, computers, or more which provide access to, or in themselves, compromise technology.

Examples: Limited-range radios for manufacturing facilities, local servers, cell phones, social media, and secure phones.

Testing equipment includes anything necessary for the successful developmental, operational, or post-repair testing of items related to a program.

Examples: Monitors, airframes, sensors, mock targets, tools, manuals, simulators, or equipment used to test the structural integrity of a system.



Information residing on internal company or Government networks, the loss or compromise of which would adversely impact classified programs.

Examples: Information on contracts, supply chains, program or materiel capability, key personnel, or processes on internal networks.

Information resident on external websites, servers, or networks, the loss or compromise of which would adversely impact classified programs.

Examples: Information on supply chain or purchasing history on vendor servers or test data remaining on monitoring equipment.

FACILITIES

Facilities are often overlooked as assets themselves, yet across the defense industrial base facilities exist which either by their capability provided or unique status would compromise or detrimentally impact military and economic superiority. Compromise of a facility can impact a program's ability to deliver materiel to the warfighter, or the USG economic advantage in a technology area.

Deciding whether a facility is a National Security Asset or a Programmatic Asset is important; classification guides and subject matter experts on the program will be good guides for those discussions.

However, if the company determines a facility to be equally important from a delivery perspective, and the same rules of consequence and likelihood are followed, a facility may be reported if it's critically important from a programmatic perspective.

This guide examines facilities in four lenses: Manufacturing, Research, Development, Testing, and Evaluation (RDT&E), those critical to Operations, and those related to Infrastructure.

FACILITIES ASSET DEFINITION

Facilities are manufacturing, research, development, testing, and evaluation (RDT&E), operations, or infrastructure related places that if compromised or incapacitated would detrimentally impact technology and programs.

- Manufacturing – Facilities directly involved with manufacturing
- RDT&E – Facilities supporting activities related to RDT&E
- Operations – Facilities directly supporting ongoing operations
- Infrastructure – Infrastructure required for critical programs

MANUFACTURING

Capability

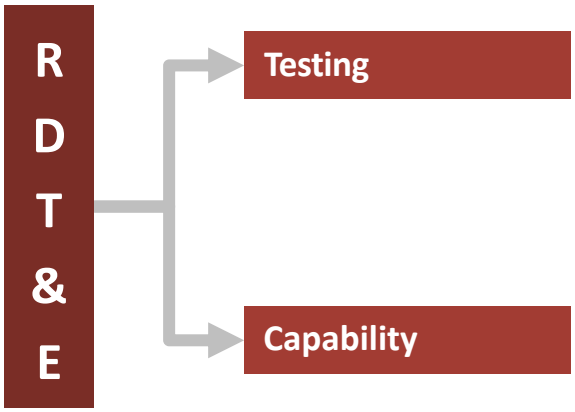
Facilities that, by design, placement, application, or use provide a capability which the loss or compromise of would detrimentally impact the technology.

Examples: Metrological calibration laboratories, hermetically sealed facilities for bio-testing, acoustic or signals analysis facilities.

Criticality

Facilities which are critical such that the loss or compromise of the facility in itself, while not a unique capability, would compromise technology or delivery.

Examples: Single point of failure facilities or facilities which alone provide the capability for the Government regardless of capability.

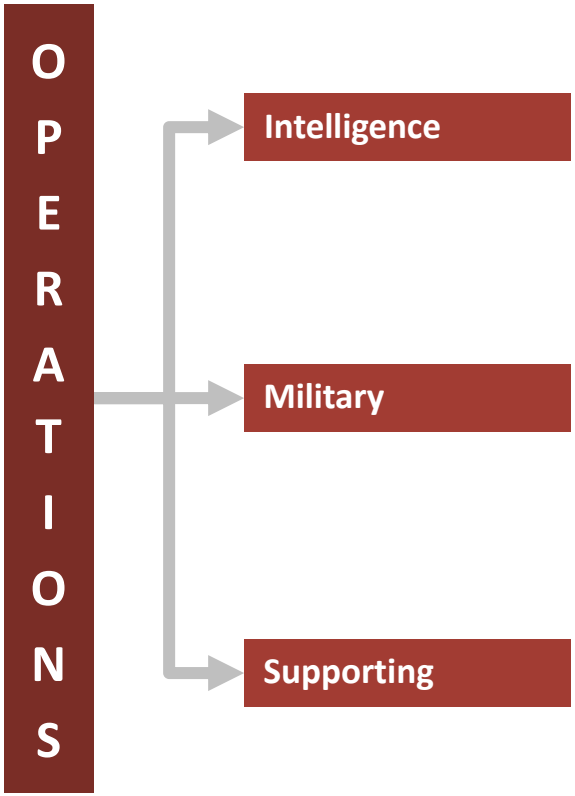


Facilities involved with testing R&D projects or materiel solutions to a degree such that the details about the facility may compromise the program.

Examples: Explosives ranges, proving grounds, detection facilities, algorithm testing, antenna test facility, aircraft systems test labs, flight test facility.

Facilities which provide valuable or unique environments or capabilities for RDT&E either by design or location which enable advances in programs and technologies.

Examples: Cold-weather testing facilities, sensor analysis facilities, acoustics facilities, shipyards, assembly plants, or sole-source, single-provider facilities.



Facilities involved with intelligence planning, tasking, gathering, evaluation, or dissemination activities and/or operations.

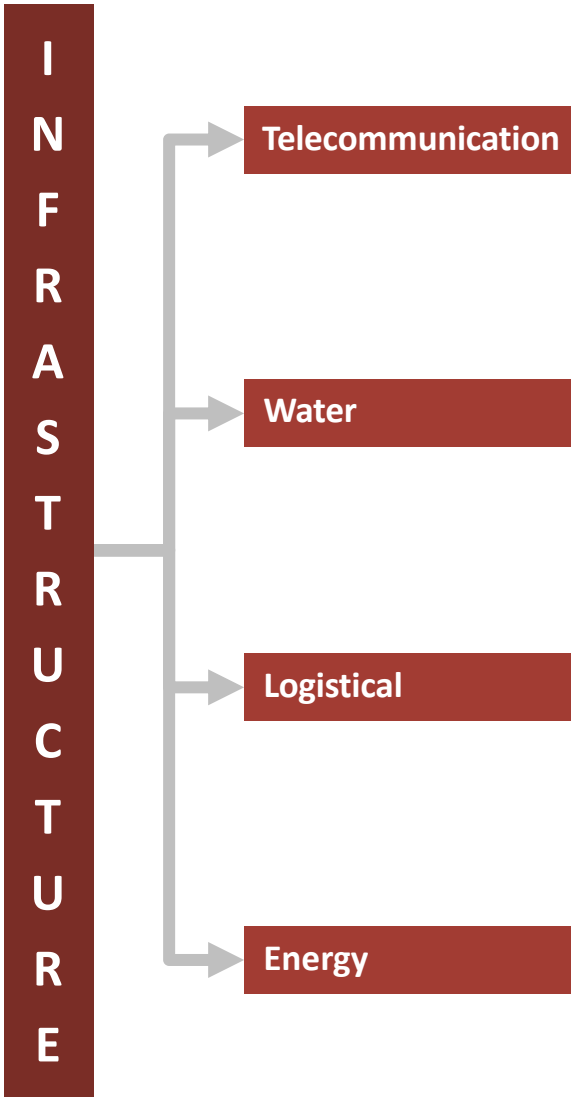
Examples: Intelligence fusion centers, contracted intelligence agency facilities, intelligence analysis or operations centers.

Facilities directly involved with supporting, enabling, or contributing to military operations, the protection of which is required to avoid compromising operations.

Examples: Airfields, supply depots, maintenance depots, shipyards, laboratories, and other industrial activities which exist outside the manufacturing sphere.

Facilities supporting operations outside intelligence or military spheres, including planning, design, engineering, training, and more.

Examples: Simulated training, contingency of operations sites or site support, mission operations support centers, warfighter field operations support centers.



Telecommunication infrastructure which enables the transmit of voice or data, carrying information relevant to the protection of the program.

Examples: Relays, cell towers, in-ground fiber, undersea cables, routers, wi-fi access points, or network cables throughout facilities.

Water infrastructure which provides access to clean water for facilities, produces ultra clean water for manufacturing, or provides critical cooling capability.

Examples: Ultra clean water facilities, desalinization plants, water pipes, data center cooling, or water quality monitoring equipment.

Logistical infrastructure which enables or supports the development, manufacture, transportation, shipment, or repair of components supporting critical programs.

Examples: Shock and vibration packaging for specialized components, safe handling requirements, or perishability requirements and timelines for shipping.

Energy infrastructure that sustains, propels, or resupplies facilities, vehicles, materiel, and personnel, either domestically or internationally.

Examples: Oil refinery, JP5 storage facilities, crude oil pipelines, power stations, backup power supplies, electrical supply infrastructure.

ACTIVITIES & OPERATIONS

Activities and Operations across the industrial base give our adversaries insight into how we train, build, supply, think, and behave. Protecting these activities and operations preserves our ability to operate in specific manners or within specific environments.

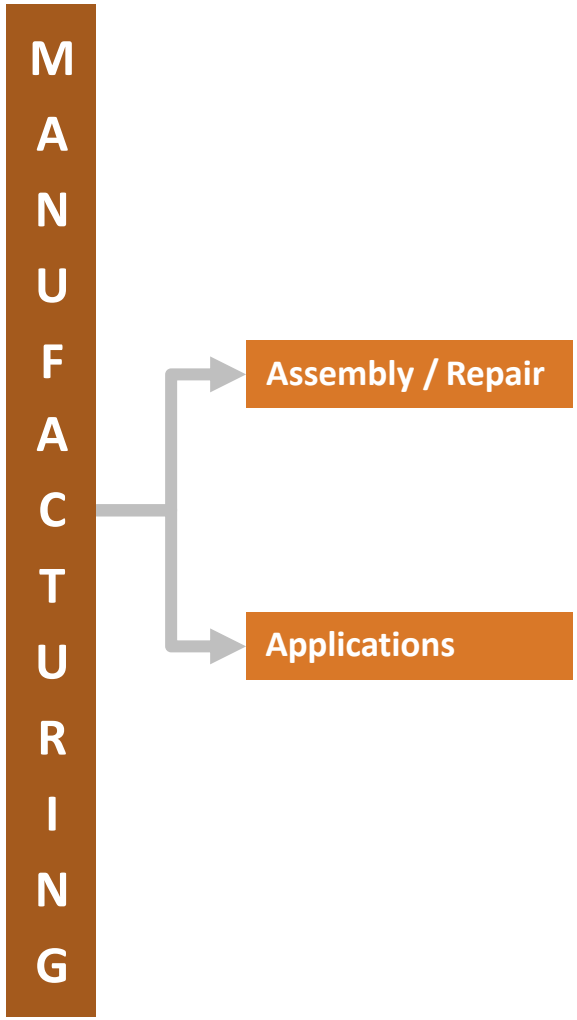
All too often, our adversaries learn our activities and operations and quickly modify their tactics, techniques, or procedures (TTPs), therein rendering our activity ineffective. Definitions herein may differ from standard DoD nomenclature.

This guide examines Activities and Operations through three lenses: Manufacturing, Intelligence, and Supporting.

ACTIVITIES & OPERATIONS ASSET DEFINITION

Activities are functions, missions, actions, or collections of actions. Operations are sequences of activities with a common theme. This guide explores activities and operations together across manufacturing, intelligence, and supporting initiatives.

- Manufacturing – Activities involved with manufacturing related to a program
- Intelligence – Activities involved with intelligence collection and analysis
- Supporting – Other supporting activities which contribute to classified programs

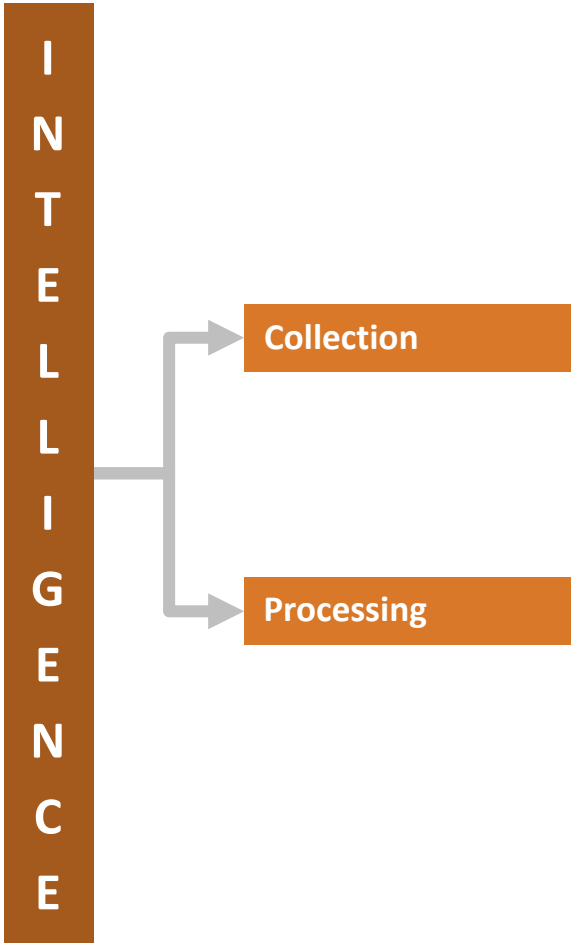


Assembly or repair activities or operations which involve final assemblies, interim components, or the maintenance or repair related to the program.

Examples: The processes involved with assembling fighter jet components or the disassembly process for a radar system.

The application of materials or coatings to the technology or any of the technology's associated assemblies or components.

Examples: Process of applying paint on airframe, or applying nonconductive materials to electronic component housings.

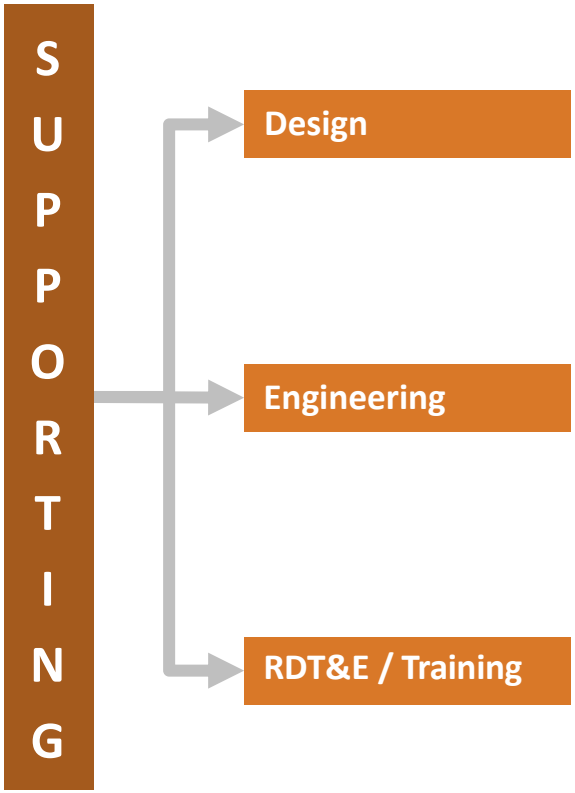


Activities or operations involved with collecting intelligence information across all traditional intelligence disciplines.

Examples: UAV tasking, collection methods, sources, operations involved with signals collection, or operations collecting communications.

Activities or operations involved with processing collected intelligence and applying new information against known conditions to create new products.

Examples: Intelligence fusion, intelligence analysis, signals analysis, or forensic, biometric, and technical exploitation of collected samples.



Design activities or operations which support equipment, systems, or materiel providing technological or strategic advantage.

Examples: Aircraft design activities, weapons design activities, propeller design and testing.

Engineering activities or operations which support materiel, platform, software, algorithm, and network development and construction.

Examples: Augmented reality, cryptography, machine learning.

RDT&E and training activities or operations which support the successful continued deployment and application of the technology.

Examples: Scenario training, test and validation activities.

SUPPLIERS

As the Government increasingly relies on Commercially developed equipment, suppliers become an increasingly difficult category to protect. The concept, design, or performance of tomorrow's capability may exist in a home office or laboratory today. The technological superiority of a future airframe may be dependent on a commercially developed compound for non-military applications.

Considering suppliers of components, expertise, or RDT&E activities can help suppress the loss and compromise of critical technologies.

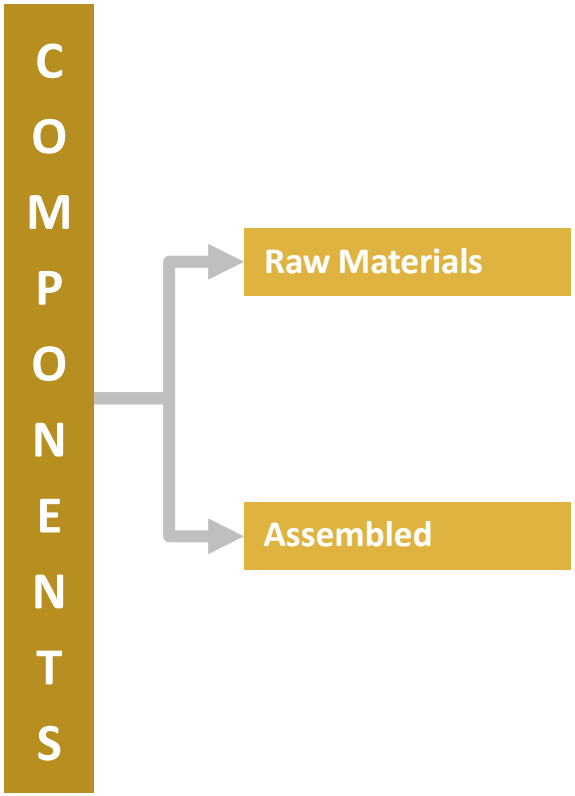
The goal when assessing suppliers is to understand whether your suppliers themselves have been vetted, have appropriate security programs, and understand where vulnerabilities exist in a supply chain such that a program can be compromised.

Identifying where suppliers are providing assets to a given program or technology is the first step in what becomes an active security program around a given supply chain.

SUPPLIERS ASSET DEFINITION

Suppliers are entities whose linked activities are associated with providing components, subject matter expertise, or RDT&E activities that if compromised would detrimentally impact programs or technologies.

- Components – Suppliers of components, either raw or assembled
- Expertise – Suppliers of expertise and knowledge
- RDT&E – Suppliers of RDT&E-related programmatic elements

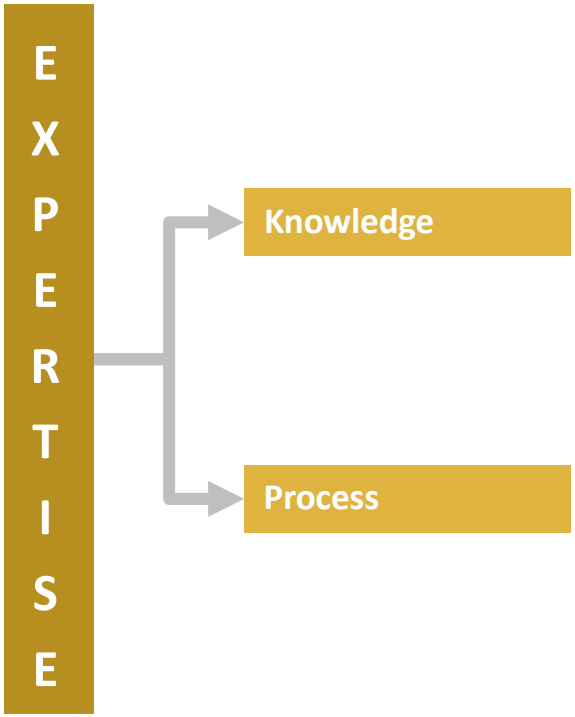


Suppliers providing raw materials as partial components or enablers for manufacturing or repair, the compromise of which would detrimentally impact the technology.

Examples: Supplier of ship-grade steel, pre-synthesized chemicals, gasses, chemically treated materials, crystal structures, or other providers.

Suppliers providing assembled components or equipment for manufacturing or repair, the compromise of which would detrimentally impact the technology.

Examples: Supplier of optical lenses, LiDAR systems, missile assemblies, vehicle armor, ballistics glass, and other assembled components.

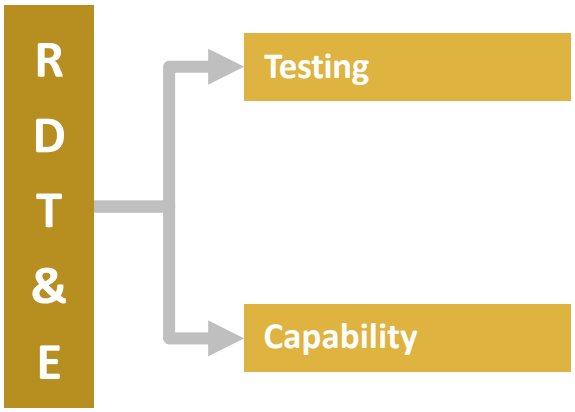


Suppliers providing knowledge or subject matter expertise in a given area to accelerate or challenge development or other activities.

Examples: Intelligence analysis, strategic planning, or foreign materiel capability.

Suppliers with processes integral to the successful development or application of a given final component or assembly to the technology.

Examples: Laser peening, chemical synthesis, chemical exploitation, or algorithm refinement.



Suppliers critical to the effective and rigorous testing of materiel solutions.

Examples: System test labs, structural test labs, composite testing, multimodal testing.

Suppliers of RDT&E capabilities which may presently fall outside the cognizance of the NISP but have the likelihood of enabling future priority technologies.

Examples: Small-scale startups, university programs, algorithm developers or outsourced programmers.

APPENDICIES

GENERAL TERMS

WORKING TERMS IPT

The general terms included in this appendix were identified by the DSS Working Terms IPT as being important to the DSS in Transition initiative. They are not necessarily used throughout the AIG.

INDUSTRIAL SECURITY

The combination of compliance and active behaviors which protect programs and technologies, prevent loss or compromise, and promote military and economic superiority.

ASSET IDENTIFICATION

The process of considering people, information, equipment, facilities, activities, operations, and suppliers which exist under the cognizance of an entity in either the context of the value they provide or the impact of their loss.

GENERAL TERMS (continued)

ADVERSARY

A state or non-state entity with capability and intent to cause harm to a valued asset.

ASSET

Anything of value related to a classified program or contract, the loss, compromise, or damage of which may adversely affect national security.

ASSET IDENTIFICATION

The process of identifying assets through which adversaries might compromise critical technologies or programs. A recurring process that starts with initial development of a Security Baseline.

COMMERCE SURVEY

An assessment survey of organizations responsible for the research, development, manufacture, test, and integration of defense and high-technology products, components, and related services conducted by the U.S. Department of Commerce (DOC), Bureau of Industry and Security (BIS), and Office of Technology Evaluation (OTE), in coordination with the Defense Security Service (DSS).

COMPROMISE

The exposure of assets, classified information, or material to an unauthorized entity.

COUNTERINTELLIGENCE

Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.

COUNTERMEASURE

An action taken or measure implemented to mitigate the exploitation or exposure of an asset through a vulnerability.

DSS IN TRANSITION (DiT)

The overarching culture change initiative to develop a new methodology for implementing an asset-focused and threat-driven approach to helping cleared facilities better protect national security information and technology.

FOREIGN INTELLIGENCE ENTITY (FIE)

Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.

IMPACT

The degree of loss or damage expected from successful exploitation of a vulnerability, measured in dollars, time, lives, supply chain consequences, operational effectiveness, or improved adversary capability.

JOINT ACQUISITION PROTECTION AND EXPLOITATION CELL (JAPEC)

A component of USD responsible for integrating and coordinating analysis to protect Controlled Technology Information (CTI) across the DoD Enterprise, thereby proactively mitigating future losses and exploiting opportunities to deter, deny, and disrupt adversaries that may threaten U.S. military advantage.

METHOD OF CONTACT

The approach used to connect an adversary to the targeted individual, information, network, or technology in order for the adversary to execute the Method(s) of Operation(s).

MISSION OWNER

An individual or entity responsible for activity related to procuring an asset for which they are the ultimate end user.

NATIONAL INTELLIGENCE PRIORITIES FRAMEWORK

A mechanism to establish, disestablish, manage, and communicate national intelligence priorities, the NIPF reflects priorities for national intelligence support and ensures enduring and emerging national intelligence issues are addressed.

GENERAL TERMS (continued)

NATIONAL SECURITY INFORMATION

Information that has been determined, pursuant to Executive Order 12958, "Classified National Security Information" or any predecessor order, to require protection against unauthorized disclosure.

PROGRAM

A directed, funded effort that provides a new, improved, or continuing materiel, weapon, information system, or service capability in response to an approved need.

PROGRAM MANAGER (CONTRACTOR)

The designated contractor individual with responsibility for and authority to execute contractor program development, production, and sustainment objectives to meet operational needs.

PROGRAM MANAGER (GOVERNMENT)

The designated U.S. Government individual with responsibility for and authority to execute program objectives for development, production, and sustainment to meet the user's operational needs.

RISK

The probability and consequence of an event causing harm to something valued (probability and severity of loss, compromise, or damage to an asset).

SECURITY BASELINE

The contractor-identified combination of critical industrial security assets under their cognizance and the associated protective measures in place at both program and asset-specific levels.

SECURITY PROGRAM

The contractor's system of security controls established to safeguard the assets in their possession or to which they have access.

SECURITY REVIEW

The process of reviewing a contractor's security program and its effectiveness to ensure the safeguards employed are adequate for the protection of identified assets.

THREAT

The intention and capability of an adversary to cause harm to an asset.

VULNERABILITY

A situation or circumstance which, if left unchanged, may result in the loss of, compromise of, or harm to an asset.

ASSET ID GUIDE QUICK LOOK

1 PEOPLE

1. Expertise
    1. Process
    2. Operations
    3. Materials
    4. Capabilities
2. Access
    1. Facilities
    2. Networks
    3. Operations
3. Influence
    1. Authority
    2. Networks

2 INFORMATION

1. Procedures
    1. Operational
    2. Technical
2. Capability
    1. Equipment
    2. Systems
3. Data
    1. Raw Data
    2. Processed Data
    3. Intelligence
4. Corporate
    1. Financial
    2. Procurement
    3. Strategy
    4. Human Resources
    5. Product

3 EQUIPMENT

1. Materiel
    1. Weapons
    2. Gear
    3. Supporting Equipment
2. Industrial
    1. Manufacturing Tools
    2. Repair Tools
3. Supporting
    1. Communications
    2. Testing Equipment
4. Network
    1. Internal
    2. External

4 FACILITIES

1. Manufacturing
    1. Capability
    2. Criticality
2. RDT&E
    1. Testing
    2. Capability
3. Operations
    1. Intelligence
    2. Military
    3. Supporting
4. Infrastructure
    1. Telecommunication
    2. Water
    3. Logistical
    4. Energy

5 ACTIVITIES & OPERATIONS

1. Manufacturing
    1. Assembly / Repair
    2. Applications
2. Intelligence
    1. Collection
    2. Processing
3. Supporting
    1. Design
    2. Engineering
    3. RDT&E / Training

6 SUPPLIERS

1. Components
    1. Raw Materials
    2. Assembled
2. Expertise
    1. Knowledge
    2. Process
3. RDT&E
    1. Testing
    2. Capability


DEFENSE SECURITY SERVICE
UNITED STATES OF AMERICA