



Asset Identification Guide: Quick Look

Primary Asset Category

People

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

Information

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

Equipment

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

Facilities

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.

Activities & Operations

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.

Suppliers

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.

Broad Asset Category

Expertise

Access

Influence

Procedures

Capability

Data

Corporate

Materiel

Industrial

Supporting

Network

Manufacturing

RDT&E

Operations

Infrastructure

Manufacturing

Intelligence

Supporting

Components

Expertise

RDT&E

Focused Asset Category

Process ◦ Operations ◦ Materials ◦ Capabilities

Facilities ◦ Networks ◦ Operations

Authority ◦ Networks

Operational ◦ Technical

Equipment ◦ Systems

Raw Data ◦ Processed Data ◦ Intelligence

Financial ◦ Procurement ◦ Strategy ◦ HR ◦ Product

Weapons ◦ Gear ◦ Supporting Equipment

Manufacturing Tools ◦ Repair Tools

Communications ◦ Testing Equipment

Internal ◦ External

Capability ◦ Criticality

Testing ◦ Capability

Intelligence ◦ Military ◦ Supporting

Telecommunications ◦ Water ◦ Logistical ◦ Energy

Assembly / Repair ◦ Applications

Collection ◦ Processing

Design ◦ Engineering ◦ RDT&E / Training

Raw Materials ◦ Assembled

Knowledge ◦ Process

Testing ◦ Capability

USING THE AIG

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.

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.

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

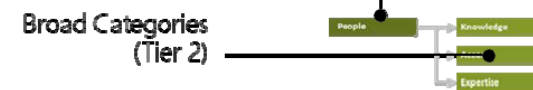
One construct to consider is whether a potential asset sits across multiple categories. This layered approach might be used to assess likelihood and consequence from multiple angles, or to compare the criticality of potential assets.

USING THE AIG



- 1 The six Tier-1, Primary Asset Categories

- 2 Primary Asset Category (Tier 1)



- 3 Broad Categories (Tier 2)

