MULTI-ASSET AND SYSTEM ASSESSMENT

OVERVIEW

The Multi-Asset and System Assessment (MASA) is an assessment process applicable to systems, campuses, and clusters. MASA collects data at the enterprise and asset levels and provides an integrated output, including criticality-ranked asset list, attack types by asset, and vulnerabilities and options for consideration.

PROGRAM DESCRIPTION

The Cybersecurity and Infrastructure Security Agency (CISA) conducts a MASA in collaboration with the infrastructure owner of the enterprise and various assets. The Protective Security Advisor leads the coordination and includes support staff from multiple organizations as needed to complete all phases of the MASA. The assessment is conducted through a series of webinars, or onsite visits, or some combination of both. Typical owner involvement includes the equivalent of 3-7 days often dispersed over a period of a couple months, but this is flexible based on the needs of the organization and availability of personnel required for the assessment.

MASA PROCESS

TABLE 1: MASA PHASES

PHASE 1	PHASE 2	PHASE 3	PHASE 4	PHASE 5
■ Approval and Preparation ■ Schedule and Pre-assessment ■ Preliminary Asset Identification ■ Background Materials	■ Enterprise-level Assessment ■ Facilitated Criticality Discussion ■ Attack Type Assignment	■ Site Visits ■ Vulnerability Assessments	■ Development of Options for Consideration ■ Draft Report	■ Final Products Development

In most cases, engagement with the following enterprise personnel (or similar titles) is required:

- Facilities manager or engineering
- Chief information officer or representative from IT
- Security manager, may include onsite law enforcement
- Human resources
- Business continuity or risk manager

Asset Criticality

The asset criticality index characterizes the criticality of each asset by considering five categories of impacts and two additional factors that affect, or modify, those impacts.

Impacts

- Operational
- Service
- Safety
- Economic
- Reputation

Modifiers

- Ease of access
- Symbolic importance

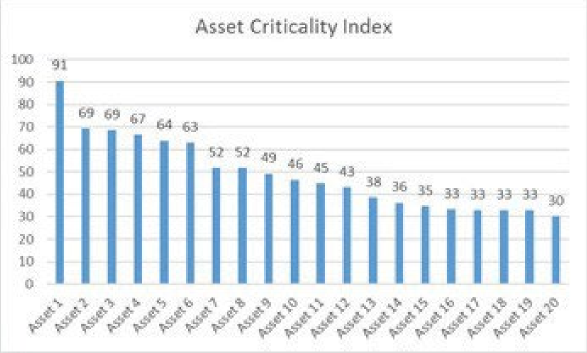


FIGURE 1. Sample Asset Criticality Ranking Graph.

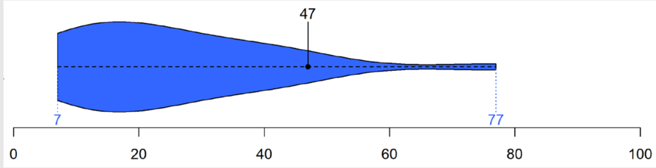


FIGURE 2. Example Criticality Distribution.

Attack Types

17 Pre-defined Attack Types | 8 Natural Hazards

Attack types are automatically assigned to each asset based on infrastructure type then adjusted as needed.

Vulnerability

- Assets are evaluated during an onsite visit, for vulnerability to each attack type
- Options for consideration are suggested to mitigate vulnerabilities

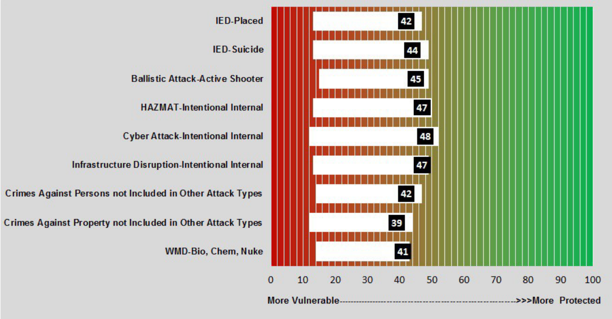
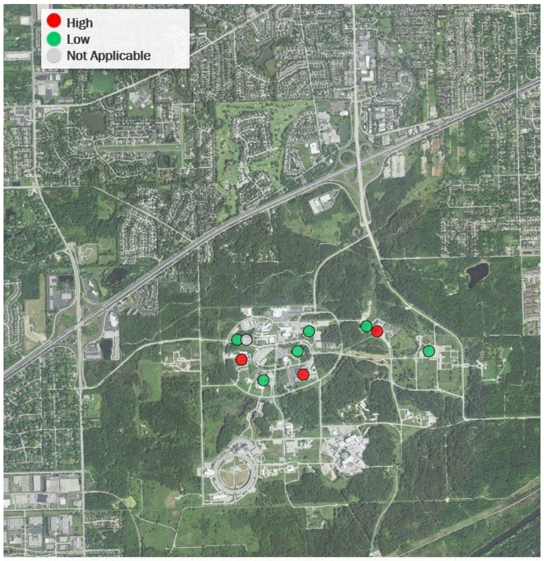


FIGURE 3. Sample Security Level Indices per Attack Type.

Product

Navigable output report containing the following:

- Enterprise and asset data
- Ranked list of assets
- Options for consideration
- Interactive maps
- Vulnerability indices
- Security and dependency dashboards



Notional data - for example purposes only

FIGURE 4. Active-shooter Threat Susceptibility.

For more information or to seek additional help, contact us at ISDAssessments@cisa.dhs.gov.