Risk-based Industrial Security Oversight (RISO)

Partnering to Protect National Security – Non-Possessor Perspective

RISK-BASED METHODOLOGY

Applying risk management principles to enhance protection

U.S. Industry leads the world in producing technologies that are the foundation of the U.S. economic and military advantage. Today, these advantages are at risk due to significant technology transfer and exploitation. Responding to this challenge, the Defense Counterintelligence and Security Agency (DCSA) has adopted an intelligence-led, asset focused, and threat-driven approach to Industrial Security. This approach utilizes a risk-based methodology to identify technologies that require the most protection, assess threats, consider vulnerabilities, and apply tailored security measures.

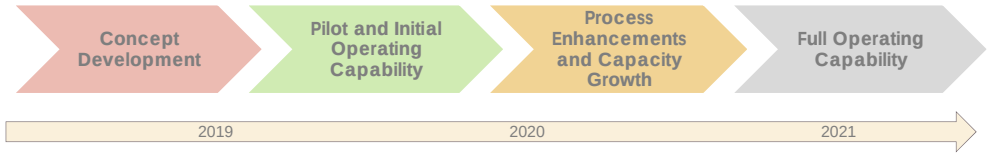
SECURITY FOR ACCESS ELSEWHERE FACILITIES

Focused oversight meeting the requirements of non-possessors

A significant percentage of facilities for which DCSA is the Cognizant Security Office are categorized as non-possessors (approximately 8,000 facilities). Traditionally, DCSA applied a similar set of requirements to both possessing and non-possessing facilities. Consistent with its shift to risk-based oversight, DCSA is forming the **National Access Elsewhere Security Oversight Center** (NAESOC) to optimize security oversight tailored to the unique requirements of selected non-possessor facilities.

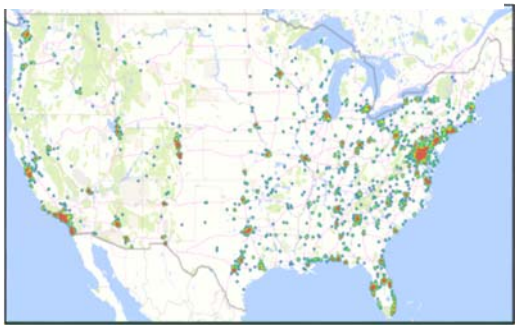
DCSA is developing thresholds to determine which non-possessor facilities meet the criteria warranting transfer to the NAESOC, and which facilities should remain assigned to traditional field offices. The NAESOC will be a centralized resource for both Government and industry partners providing communications and oversight for non-possessor requirements and issues. The relationships and processes created by this new oversight center will optimize communications, threat reporting, and changes to facility profiles that will allow early risk-informed decisions by Government Partners.

Timeline for NAESOC development and implementation



Operational view of NAESOC when implemented

Geographic Distribution of Non-Possessors



NAESOC Methodology

Centralized oversight provides a common operating picture for facilities with unknown risk and efficiently informs all stakeholders

DCSA and Industry Partnership

As DCSA's security oversight approach evolves from a primary focus on National Industrial Security Program Oversight Manual compliance to critical technology protection, Industry will serve a key role.

Facility Security Officers should be able to:

- ✓Identify critical assets at their facility and the security controls in place to protect each asset
- ✓Document business processes and supply chains
- ✓Develop Tailored Security Plans (TSP) identifying effective security controls and countermeasures
- ✓Monitor effectiveness of Tailored Security Plans

DCSA and Government Partnership

With this shift in focus, the Government role becomes increasingly essential to:

- ✓Establish GCA risk priorities
- ✓Determine which facilities require NAESOC oversight
- ✓Identify vulnerabilities and priority changes

Partnership with GCA will:

- ✓Increase information exchange on program priorities and critical technologies
- ✓Assess risks from identified vulnerabilities
- ✓Focus on measures to ensure contracted capabilities are delivered uncompromised

"This threat is unparalleled in our nation's history and directly affects everyone in this country." Daniel Payne, Director DCSA

Version 1c, Jun 2019