# OPERATIONS SECURITY (OPSEC)

JULY 2022

THIS PRODUCT WAS PUBLISHED BY THE NCSC'S ENTERPRISE THREAT-MITIGATION DIRECTORATE & THE NATIONAL OPERATIONS SECURITY PROGRAM (NOP) OFFICE

# National Operations Security Program Critical Information List Job Aid

## Purpose

This Operations Security (OPSEC) Critical Information List (CIL) job aid provides areas of awareness and direction for developing an organization's CIL. This guidance is not limited to this list and additional critical areas should be considered when drafting a tailored CIL for your organization.

## Developing a CIL

This guidance is designed to provide areas of awareness and direction for developing an organization's CIL. This list is not all-inclusive, nor universally applicable. Additional critical areas should be considered when drafting a tailored CIL for your organization. The keys to developing a CIL are to 1) identify real and potential adversaries, and to 2) recognize how the disclosure of particular facts or data could increase risk.

The organization should have several critical information lists that correspond to each of the organization's levels. The following exemplifies a potential set of CILs for an organization:

- Organization CIL: An overall critical information list that contains items vital to the success of the organization.
- Division CIL: Each division should have a CIL that supports the Organization CIL and contains items vital to the success of the division.
- Element CIL: Each element should have a CIL that supports the Division and Organization CILs and contains items vital to the success of the element.

## Characteristics of a Good CIL

The CIL is designed so that everyone understands what information is critical and should be protected. Remember, the purpose of the CIL is to focus on *unclassified* information that is sensitive and critical to the success of an organization or mission.

Everyone understands that classified information must be kept confidential, but they may not realize unclassified information should also be confidential and protected. Additionally, as noted in Executive Order

13526, Section 1.7.(e): "Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information."

Following are characteristics of a good, effective critical information list:

- The CIL should be based on an upper-echelon CIL that already exists.
- The CIL should be short and contain no more than 10 or 15 items.
- The CIL should contain only sensitive, unclassified items.
- The CIL should be easy to read and use terms that everyone understands.
- The CIL should be approved by senior leadership.
- The CIL should display the date it was created and approved.
- The CIL should be widely disseminated within the organization, division, or element.

## Examples of Critical Information

Remember, a critical information list should describe information that is critical to both your organization's or mission's success, as well as to the adversary's success. The items on your critical information list may fall into one of the following categories:

**Manpower and Personnel:** Exact number of personnel assigned to an organization; exact number of assigned personnel with specific skillsets or certifications; personal identifiable information; travel itineraries; employees' work schedules; and meeting agendas of senior leaders; and organization charts.

**Security:** Security classification guides; numbers and identities of personnel with security clearances or access to special programs; security procedures; and security vulnerabilities.

**Strategy/Plans/Policy/Operations:** Information related to operations, activities, and investments, including strategic plans, operational plans, lessons learned, contingency plans, inspection results, concepts of support, courses of action, exercises, mishaps, and accidents prior to authorized official public release; standard operating procedures; decisional capabilities, vulnerabilities, and organizational readiness information.

**Medical:** Personal health information; maintenance/supply capabilities and vulnerabilities; and shortages of medical supplies/personnel.

**Budget and Contracting:** Budgetary information and allocations relating to gains, losses, shortfalls, unfunded requirements, and issue papers; pre-contract award information; supply chain details; locations/specifics of contract duty; contractor information or service-sharing agreements with other private organizations and

companies projected to be involved in sensitive and new and emerging technology acquisitions; and specific contract requirements.

**Research and Development:** Budgetary information related to R&D funding for new and emerging technology; new or existing technologies, supply chain assessments and academia reviews; R&D projects to address vulnerabilities in current technologies, Artificial Intelligence algorithms, training data, capabilities and limitations, unclassified database locations used by the R&D community; and specific contract criteria associated with R&D activities.

**Communications and Infrastructure:** Information related to critical infrastructure, including wireless communications and computer network systems; information technology vulnerabilities; and communication limitations.

**Organizational Development:** Information related to organizational efforts to develop capabilities, and organizational models, and determine/document organizational authorities for future plans and programs; and details regarding specialized training for personnel with specific skillsets or certifications.