Critical Information Lists (CILs)

Security+ YOU — Think. Assess. Protect.

All Members of the Workforce (MOWs) are responsible for **practicing good OPSEC** (aka operations security) by protecting critical information from inadvertent or intentional release outside of the security boundary, where it can be **exploited by an adversary** intent on harming Sandia, our allies, or our mission.

Critical information at Sandia is **specific facts** about friendly intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences of accomplishment of friendly objectives.

At Sandia, critical information must be identified at the programmatic or operational level. The OPSEC program oversees the identification of the critical information and assists MOWs in analysis of factors including risk, consequence of loss, and adversary (e.g., insiders, foreign intelligence entities, violent extremists, etc) intent and capability.

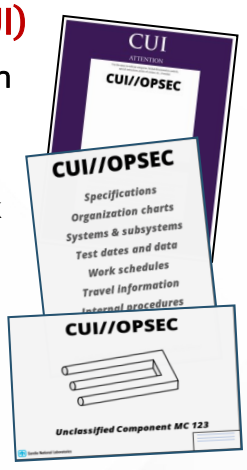
Using a *Critical Information List (CIL)*

Once identified, critical information is compiled into a **Critical Information List (CIL).** All approved CILS are published in the Critical Information List Library. You are required to maintain an understanding of all CIL(s) that apply to your work.

A CIL provides any MOW with a concise listing of critical information topics that must be protected against inadvertent or intentional release. A CIL will often include topics that you do not believe are sensitive - if identified on a CIL, that information is **valuable to an adversary** and must be protected. A CIL may also include additional countermeasures against release, such as procedures to prevent sensitive information from being released via aerial imaging during outdoor activities

Review the most current CILs relevant to the work you do by visiting the Critical Information List Library on the OPSEC homepage on the Sandia Restricted Network (SRN). Without SRN access, request a copy of any appropriate CIL(s) from your manager.

Protecting critical information as **Controlled Unclassified Information (CUI)**



All MOWs are responsible for identifying and protecting **Controlled Unclassified Information (CUI).** Government-owned unclassified information that is addressed in a CIL is controlled as **CUI** according to the Operations Security category, and is marked **CUI//OPSEC.**

When reviewing your information for CUI, any information identified on a CIL for your work is CUI, and **must be protected**. As critical information is CUI, it must be removed prior to publishing or releasing information where it can be exploited by an adversary.

If you encounter information that you believe to be useful to an adversary (e.g., critical information) that is not addressed in a CIL relevant to your work, contact Sandia's OPSEC Program to begin development of a new CIL or to update an existing CIL.

For more information, contact Sandia's OPSEC Program at opsec@sandia.gov, or visit the OPSEC Program homepage at opsec.sandia.gov on the SRN.

NNSA National Nuclear Security Administration — U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

SAND2023-01729O 03.29.2023 v1.0

Sandia National Laboratories