

Information Security Oversight Office

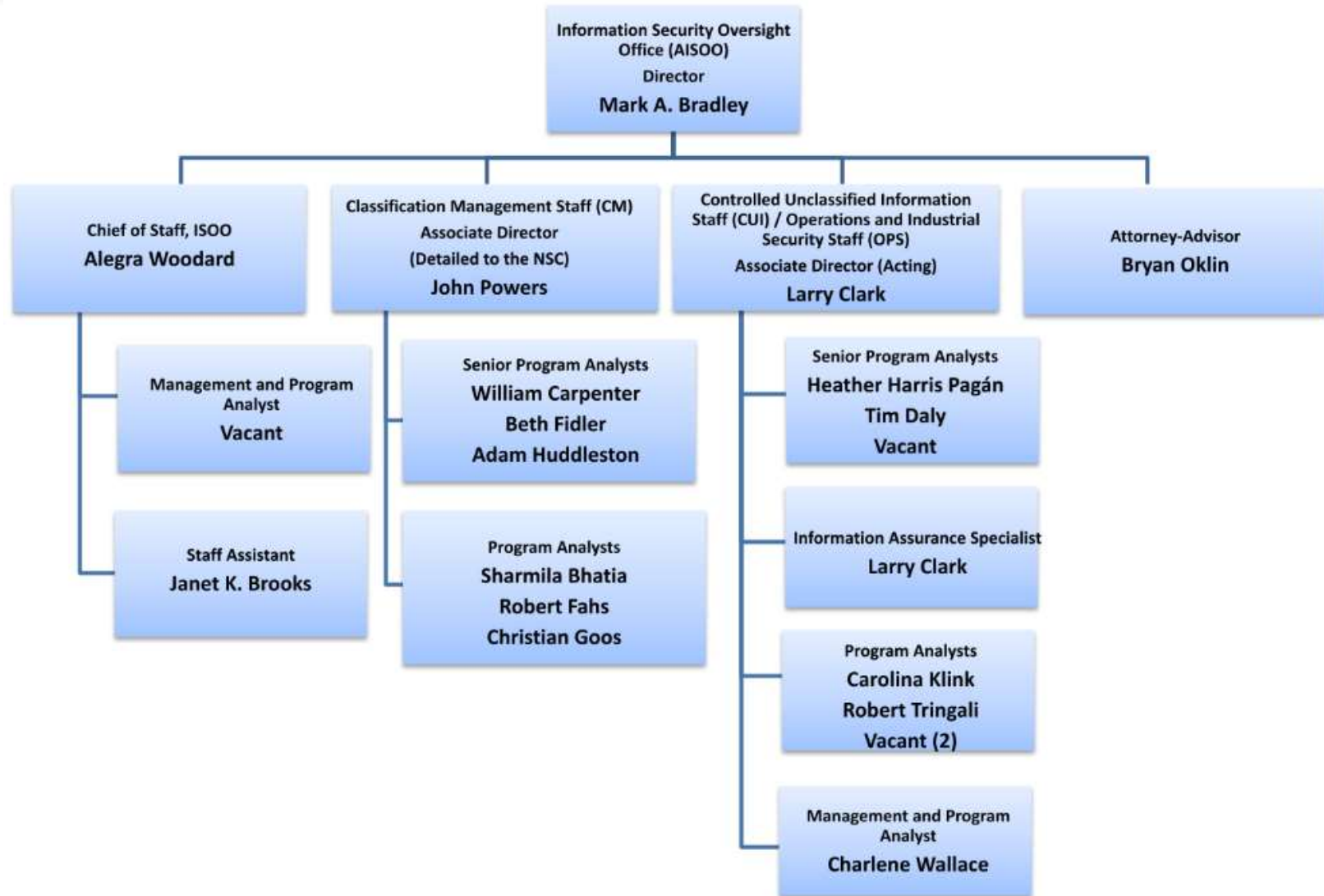
Protect • Inform • Assess



Agenda

- NSC Memo
- CUI
- Safes
- References
- Contact Information

ISOO's Organizational Chart



NSC Memo

- NSC Memo “Initiating a Process to Review Information Management and Classification Policies, 6/2/2022
 - An Interagency Policy Committee (IPC) will review Executive Orders (EO) 13556, CUI and EO 13526, Classified National Security Information (CNSI)
 - CUI Notice 2022-01
 - Guidance Regarding Memo

What's Next for CUI

- **Implementation Efforts Continue**
- **CUI Federal Acquisition Regulation (FAR) Clause**
- **Information Security (IS) Systems**
 - Federal Information Processing Standards (FIPS) Publication 199
Moderate Confidentiality Impact Level
 - National Institute of Standards and Technology (NIST) Special
Publication (SP) 800-171
- **Cybersecurity Maturity Model Certification (CMMC) is a DoD-
mandated program, not IS00**

CUI FAQs

- **Q: Who is authorized to label something CUI?**
- **A: Contractors need to follow what is in their contract. CUI requirements do not bind the public, except as authorized by a law, regulation, or as incorporated into a contract or agreement. They are authorized to mark CUI information, however, they can only do it when instructed to do so in the contract or supporting documentation, and have a lawful government purpose to do so.**
- **Q: What are the types of information that can be CUI?**
- **A: The CUI Registry contains a list of different types of CUI. It can be found at <https://www.archives.gov/cui/registry/category-list>.**

CUI FAQs

- Q: How can CUI be sent?

- Authorized holders must follow their contract's guidelines, however, some options are:
 - May use the United States Postal Service or any commercial delivery service;
 - Should use in-transit automated tracking and accountability tools;
 - May use interoffice or interagency mail systems; and
 - Must mark packages that contain CUI according to marking requirements

CUI FAQs

- **Q: How does CUI have been be stored electronically?**
- **A: In accordance with FIPS PUB 199, CUI Basic is categorized at no less than the moderate confidentiality impact level. FIPS PUB 199 defines the security impact levels for Federal information and Federal information systems. Appropriate security requirements and controls from FIPS PUB 200 and NIST SP 800-53 must be applied to CUI in accordance with any risk-based tailoring decisions they make.**
- **Agencies may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements with agencies or non-executive branch entities (including agreements for the operation of an information system on behalf of the agencies). Agencies may not otherwise require controls for CUI Basic at a level higher or different from those permitted in the CUI Basic requirements when disseminating the CUI Basic outside the agency.**

CUI FAQs

- **Q: How can CUI be stored in the physical environment?**

- **A: Authorized holders must take reasonable precautions to guard against unauthorized disclosure of CUI. They must include the following measures among the reasonable precautions:**
 - Establish controlled environments in which to protect CUI from unauthorized access or disclosure and make use of those controlled environments;

 - Reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations discussing CUI;

 - Keep CUI under the authorized holder's direct control or protect it with at least one physical barrier, and reasonably ensure that the authorized holder or the physical barrier protects the CUI from unauthorized access or observation when outside a controlled environment.

CUI FAQs

- **Q: How can CUI be destroyed?**

- **A: It must be done in a manner that makes it unreadable, indecipherable, and irrecoverable. Entities must use any destruction method specifically required by law, regulation, or Government-wide policy for that particular CUI. If the authority does not specify a destruction method, agencies must use one of the following methods:**
 - **Guidance for destruction in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800-88, Guidelines for Media Sanitization or**

 - **Any method of destruction approved for Classified National Security Information.**

CUI FAQs

- Q: Can a contractor call CUI information proprietary?
- A: Any information received or created as part of a current or previous contract should be protected in accordance with the terms of the contract under which it was received or created. As agencies implement, CUI requirements will be added to existing and new contracts.
- Q: Who should they go to with questions on CUI?
- A: Any of the below:
 - Their Government Contracting Activity (GCA)
 - Cognizant Security Agency via the appropriate company POC
 - CUI team at ISOO

Red Label GSA Approved Containers

- Notices about Transition
 - ISOO Notice 2021-01
 - ISOO Notice 2022-03
- Only Approved Method to Order GSA Containers is through GSA
- Cannot Order Through Third Parties
- Reference pptx and pdf provided for step by step instructions

References

- **CUI Marking Handbook**
 - <https://www.archives.gov/cui>
- **Collateral Classified Marking Handbook**
 - <https://www.archives.gov/isoo/training/training-aids>
- **Public Interest Declassification Board (PIDB) Recommendations and Reports**
 - <https://www.archives.gov/declassification/pidb/recommendations>
- **ISOO Notices**
 - <https://www.archives.gov/isoo/notices>
- **CUI Notices**
 - <https://www.archives.gov/cui/registry/policy-guidance#directives>
- **CUI FAQs**
 - <https://www.archives.gov/cui/faqs.html>

Contact Information

- **General**

- <https://www.archives.gov/isoo>
- <https://isoo-overview.blogs.archives.gov/>
- ISOO@nara.gov

- **CUI Questions**

- CUI@nara.gov
- <https://www.archives.gov/cui>
- <https://isoo.blogs.archives.gov/>

- **National Industrial Security Program (NISP) Questions**

- NISPPAC@nara.gov
- 202-357-5351

- **State, Local, Tribal, Private Sector (SLTPS) Questions**

- SLTPS_PAC@nara.gov
- 202-357-5351