

VA Privacy Service

Brown Bag Webinar Series

Event Resource Guide

On behalf of the U.S. Department of Veterans Affairs (VA) Privacy Service, thank you for participating in the Privacy in Action Brown Bag Webinar Series event, “Lunch and Learn: VA Privacy Today.” We hope you found the information presented by our presenters insightful and meaningful to your daily work. Below is a recap of the main topics discussed today with links to additional information.

Social Security Number Reduction

In 2007, the Office of Management and Budget (OMB) issued memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, requiring agencies to review their use of Social Security numbers (SSNs) in agency systems and programs to identify instances in which the collection or use of the number was unnecessary. Lastly, the memorandum required agencies to explore alternatives to using SSNs as personal identifiers for Federal employees and in Federal programs.

VA is committed to safeguarding Veterans' and employees' privacy by reducing or eliminating the use of SSNs in records. VA's SSN Reduction Initiative is an ongoing program, initiated by OMB Memorandum 07-16 and driven by other Federal legislation such as the [Social Security Number Fraud Prevention Act of 2017](#) and the [Consolidated Appropriations Act, 2018, \(Sec. 240\)](#).

RESOURCES

- SSN Reduction Privacy Hub
 - <https://vaww.vashare.oit.va.gov/sites/PrivacyHub/SitePages/SSN%20Reduction.asp>
[X](#)

Controlled Unclassified Information

Controlled Unclassified Information (CUI) is unclassified information that requires safeguarding or dissemination controls pursuant to a law, regulation, or government wide policy. This includes information that you all handle regularly, such as health and privacy information, but it also includes personnel records, financial and acquisition information, and even information related to physical and electronic security. Executive Order 13556, Controlled Unclassified Information, established the CUI Program.

The CUI Program is a federally mandated program that establishes standardized practices for protecting sensitive information across more than 100 departments and agencies; state, local, Tribal, and private sector entities; academia; and industry. The goal of the program is to enable



U.S. Department of Veterans Affairs
Office of Information Technology

VA Privacy Service

Brown Bag Webinar Series

Event Resource Guide

timely and consistent information sharing across these entities and to increase transparency throughout the Federal government and with non-Federal stakeholders.

RESOURCES

- VA CUI Intranet Site
 - <https://vaww.oit.va.gov/services/cui/>
- NIST Proposes Draft Enhanced Security Requirements for Protecting CUI
 - <https://www.natlawreview.com/article/nist-proposes-draft-enhanced-security-requirements-protecting-cui>
- CUI Awareness
 - <https://www.youtube.com/watch?v=4Bq9tPxp6WY&feature=youtu.be>

Data Loss Prevention

Data Loss Prevention (DLP) is a VA enterprise wide program with the mission to prevent unauthorized exfiltration (data loss) of Veterans and VA sensitive data by a user or a system. To accomplish this mission, DLP works directly with VA Privacy Services and other key stakeholders in OIS and OIT to:

- Protect VA's reputation/brand—DLP will enhance VA's support of Veterans by reducing VA's data exfiltration risk.
- Add to VA's existing security architecture—With the customized Baseline Model and Use Case assessments, DLP will strengthen existing VA security infrastructure and capabilities.
- Encourage a mindset for data protection—DLP will work with VA Privacy Service to help everyone be aware and act to prevent unauthorized data loss.
- Deepen and expand VA's security platform—By updating/adding DLP policies and implementing enterprise DLP protection programs, VA will minimize vulnerabilities.

RESOURCES

- DLP Fact Sheet
 - https://vaww.oit.va.gov/wp-content/uploads/2020/07/DLP_FactSheet_Final-Approved_07_10_20.pdf
- Contact information for DLP
 - VADLPPROGRAM@va.gov



**PRIVACY
MATTERS**

**PRIVACY
BUILDS
TRUST**

VA



U.S. Department of Veterans Affairs
Office of Information Technology

VA Privacy Service

Brown Bag Webinar Series

Event Resource Guide

- What is Data Loss Prevention (DLP)? A Definition of Data Loss Prevention
 - <https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention>
- Cloud Data Loss Prevention Market is Staring at a Promising Future Owing to High Demand for 2017 – 2025
 - <https://newsbrok.com/uncategorized/39128/cloud-data-loss-prevention-market-is-staring-at-a-promising-future-owing-to-high-demand-for-2017-2025/>

Event Question & Answer:

- **Will the handouts or slide be made available such as DLP assessment Use case**
 - You can access any of the DLP Use Case Assessment reports at [DLP Sharepoint](#). At the DLP Sharepoint home, scroll down and click on the link [Use Case Reports](#) and you can review any of the final Use Case Assessment reports. If you have any further questions, do not hesitate to reach out and contact the DLP team at: VADLPPROGRAM@va.gov.
- **Does DLP Program address removable media? USB/CD/DVD etc.**
 - Yes, we will. VA currently does have a Removable Media Solution that whitelists authorized devices for a temporary time period and blocks all other non-authorized removable devices.
- **Is there a dashboard in place used to monitor attempted exfiltration attacks?**
 - Yes, the VA Office of Information Security (OIS) is developing a host of different dashboards to monitor the security posture of the VA. The DLP Program is working along with OIS to develop dashboards specifically geared towards Data Loss Prevention.
- **Has the CUI Program been engaged with the CIO/ESO staff in order to address NIST Controls in eMASS (VA's Governance Risk Compliance) tool for Systems/Areas of record? NIST Security-Privacy Control MP-8(3) calls for CUI to be defined and downgrade instructions to be applied to local media (PII/PHI redaction/de-identified), however, this control is currently being addressed as not applicable at the Area level in eMASS.**
 - Until the CUI directive/policy is published we cannot implement changes to the controls applied to VA systems, therefore this control will remain not applicable until that time. However, the CUI Team is working closely with Privacy and other groups within OIS to discuss how these controls are being addressed in the interim and how the CUI Program will impact controls in the future.



PRIVACY
MATTERS

PRIVACY
BUILDS
TRUST

VA



U.S. Department of Veterans Affairs
Office of Information Technology

VA Privacy Service

Brown Bag Webinar Series

Event Resource Guide

- **Will Records Management Officers (RMOs)/Privacy Officers be involved in CUI program? What will our role be?**
 - RMOs and Privacy Officers will play a key role in implementing the CUI Program because of their valuable experience protecting and managing information that will be considered CUI in the future. We are currently working closely with Records Management and Privacy leadership to understand current practices for handling and protecting information to ensure CUI policies and processes will integrate without impacting VA's mission. More information and guidance will be provided to RMOs and Privacy Officers in the future once the CUI Program is ready to deploy across the agency.
- **As PAPER is reduced or completely removed from some processes, How do you mark files as CUI?**
 - The marking requirements for CUI are the same for physical and electronic documents that contain CUI. Further guidance on how this information will be marked will be provided through a CUI handbook and training course in the future.
- **I've heard drive mapping will take place soon, will this be part of the CUI program? Can you speak more on this?**
 - The CUI Program is not responsible for drive mapping at this time.



U.S. Department of Veterans Affairs
Office of Information Technology