# Operating Experience Summary

OES 2025-06 June 2025

# Managing Controlled Articles in Security Areas

## Purpose

This Operating Experience Summary (OES) raises awareness of potential security vulnerabilities across the Department of Energy (DOE) Enterprise related to the presence of recording and transmittal devices in security areas. The prevalence of devices such as smartwatches, cameras, microphones, and Bluetooth medical devices in our lives continues to increase, presenting an evolving threat that requires additional diligence in establishing robust processes and verifying effectiveness of controls. The OES shares examples from the field, lessons learned, and recommendations that can support risk reduction.

## Background

Over the past several years, the Office of Enforcement identified a trend in the number of incidents of security concern (IOSC) involving unauthorized/unapproved controlled articles with prohibited technologies being introduced and remaining for long periods in areas where classified information is processed, used and stored, as well as in areas where classified discussions are permitted. As technology advances and the need for wearing medical devices increases, the number of incidents continues to rise (both reported and unreported). Federal and contractor management must devise solutions to counter this increasingly prevalent problem.

### Controlled Articles

Portable electronic devices (PED), both Government and personally owned, **capable of recording information or transmitting data** (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment) are not permitted in Limited Areas (LAs), Protected Areas (PAs), and Material Access Areas (MAAs), without prior approval documented in the approved Security Plan (SP).

Examples include:

- Wireless headsets and keyboards
- Smartwatches, Smart TVs
- Two-way radios
- Some medical devices
- Anything with Wi-Fi and Bluetooth

## Operational History

The presence of recording and transmitting devices in areas where classified matter is present, or classified discussions occur poses the risk of the unauthorized disclosure of this information. As we all are aware, there is a much greater reliance on the use of personal and government-owned electronic devices by members of the workforce. Items such as cell phones, tablets, and laptops are all equipped with audio and video recording capabilities and can transmit this information. The presence of Bluetooth technology is increasingly found in all types of devices (e.g., watches, tennis shoes, coffee pots, cups, etc.). In some cases, personnel may not be aware that these devices have this capability. In other cases, the presence of unauthorized controlled articles in security areas was due to a lack of security education or awareness, or even a willful disregard of security requirements.

**The following field experience examples illustrate some of the security concerns:**

Example 1: A member of the workforce installed two test cameras inside a vault-type room (VTR). The cameras were aimed at computer terminals authorized to process classified information. As part of the test activities, video recordings of these terminals were streamed over an unclassified network. Although reported to the site IOSC program, no inquiry was performed, and the cameras were allowed to remain in place for over a year. When the incident was reported a second time, an inquiry was conducted, and the cameras removed. As part of the corrective actions a cursory walk down of all VTRs on site was conducted whereupon dozens of unauthorized/unapproved controlled articles were discovered.

Example 2: Another incident involved the presence of unauthorized/unapproved controlled articles inside a security space with strict access controls where classified information was used, stored and processed. Because of these access controls, the manager of the employees working in this space did not have authorization to enter the area without first notifying the employees who would then allow him access. As a result of this loss of management control, the employees brought unauthorized controlled articles into the area and violated other information security requirements.

Example 3: An employee accidentally discovered that their government laptop microphone was active and recording and not disabled as they thought. Although the laptop had been purchased in accordance with procurement processes requiring the vendor to physically disable all prohibited technologies (i.e. microphone/camera/Bluetooth), the microphone had not been disabled and had been inside the security area for more than one year. A broader Site review identified additional laptops with this same issue.

**Other Office of Enforcement observations included:**

- Inconsistent reporting and investigation of incidents involving personal and government cell phones being brought into security areas. In some cases, whether an IOSC inquiry is performed and/or reported depends on the amount of time the device was in the area (e.g. a few minutes to several hours) or if classified activities were in the vicinity of the device (which ranges from independent verification by the inquiry official or merely asking the person if they were aware of any classified processing or discussions).
- Inconsistent line management responsibilities identifying the presence of unauthorized controlled articles in security areas. These responsibilities range from doing an annual review of approved controlled articles to little or no responsibilities in this area.
- Failure to remove controlled articles from security areas once the justification for approval is no longer required. Very few sites have any provision for removing controlled articles from security areas once the purpose of having the article in the area has been served. One site establishes a one-year authorization limit for all approved controlled articles to be renewed annually; however, the policy does not define who will conduct this annual authorization and therefore the controlled article remains in the security area indefinitely.

## Lessons Learned and Recommendations

**Verify that processes and procedures are effective through self-assessment.**
DOE Order 473.1A, *Physical Protection Program*, requires that policies and procedures be established to deter the introduction of unauthorized and unapproved controlled articles in areas with access to classified information. However, based on current observations, additional effort in self-assessment can help ensure these processes/procedures are clear, effective, and consistently implemented.

- Many information security related self-assessment activities focus on marking of classified documents and the completion of forms associated with security containers.

- Ensure the self-assessment program scope includes an evaluation of whether unauthorized controlled articles are present in security areas. Include physical security personnel for inspections of physical spaces.
- Random verification of policy/procedure implementation could also be performed by managers/supervisors, embedded security personnel within organizations or by CMPC personnel as part of their assessment activity.

**Review site approved procedures and plans for adequate rigor in implementing the DOE policy.**
DOE Order 473.1A, Attachment 2, Chapter III.1.b requires each site to establish procedures and processes to address the authorization and approval of controlled articles. In some cases, the measures range from a rigorous program based on applicable risk to one that has minimal rigor that could leave the risk determination to the individual employee.

- Do the approved plans ensure that the appropriate rigor is identified based on the identified risk and facility assets?
- Does the Security Plan include an expectation and a defined process to perform periodic checks for prohibited and controlled articles?
- Is the Security Plan clearly tied to the results of the site risk-assessment?

**Participate in DOE complex-wide Communities of Practice (CoPs) and Working Groups (WGs) to share good practices for control measures and risk reduction.**
Sites may be challenged to address the vulnerabilities created by controlled articles with recording and transmitting capabilities and the potential of unauthorized disclosure of classified information. This challenge is ever evolving due to continuous changes in technology. Existing WGs, such as the Physical Protection Systems Policy Panel (PPSPP)[1], the Energy Facility Contractors Group (EFCOG) Safeguards & Security WG, and the Center for Security Technology, Analysis, Response and Testing (CSTART)[2] can provide a central communication platform to raise issues and facilitate the sharing of lessons learned and helpful operational practices among sites.

- Topics to be addressed could include the use of medical devices, engineered measures to detect the presence of devices capable of transmitting data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment), incident reporting guidelines, and disciplinary measures for multiple offenders to name a few.
- Other areas for consideration include lists of recommended devices or equipment (those that do not pose unnecessary risk) and devices that should not be purchased due to the difficulty in mitigating inherent vulnerabilities.

**Reinforce the use of human performance improvement (HPI)[3] tools for error prevention.**

- Review the effectiveness of signs in security areas to draw the employee's attention.
- Consider automated means to alert employees before entering a security area that they may have a controlled article on their person.
- Provide refresher training to ensure employees understand security entry screening expectations related to new technology. Employee self-check prior to entry is the last defense!

---

[1] The PCSPP is one of several Working Groups (WGs) led by the EHSS Office of Security Policy. It provides a forum for physical security practitioners across the DOE complex to discuss security issues, share lessons learned, make recommendations, and provide input to future policy revisions.
[2] CSTART is a virtual clearinghouse managed by the National Nuclear Security Administration (NNSA) with the goal of improving connectivity and communications across the NNSA safeguards and security program. CSTART is open to S&S professionals throughout the Department and requires registration for an account.
[3] HPI considers individual and leader behaviors for the reduction of error, as well as improvements needed in organizational processes and values and job-site conditions to better support worker performance. [DOE-HDBK-1028-2009, Volume 1]

The following Lessons Learned articles were published in DOE OPEXShare for use by the DOE Enterprise:

**DOE OPEXShare Lessons Learned**

The links to these Lesson Learned articles require a DOE OPEXShare user account. You can register here.

- Laptop Computers with Recorders (Nevada National Security Sites, May 2024)
- Prohibited and Controlled Articles (PACA) Introduced into Limited Areas (LA) (SRPPF) (Savannah River Nuclear Solutions, September 2023)
- Controlled Articles (Oak Ridge National Laboratory, May 2023)
- Government-Issued and Personal Cell Phone Recording Device or Cameras May Present Vulnerabilities (Nevada National Security Sites, February 2023)
- Understand Security Requirements Before Moving to a New Location (Lawrence Livermore National Security, February 2023)
- There is NO Room for Complacency When Performing Secure Area Escorting Duties (Nevada National Security Sites, September 2021)
- Accepting Unnecessary Risks (Pacific Northwest National Laboratory, November 2020)
- Systemic Failures Resulted in the Inadvertent Introduction of Prohibited Article into Unauthorized Area (Nevada National Security Sites, August 2020)

## Requirement References

DOE O 473.1A, Attachment 2, Chapter III.1.b states “Sites are to develop procedures to deter the introduction of prohibited and controlled articles. These procedures must be documented in a Security Plan (SP) approved by the Officially Designated Federal Security Authority (ODFSA).”

DOE O 473.1A, Attachment 2, Chapter III.3.a. states “Controlled articles such as portable electronic devices (PED), both government and personally owned, capable of recording information or transmitting data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment) are not permitted in LAs, VTRs, PAs, and MAAs, without prior written approval.

1. The approval process permitting controlled articles must be documented in the approved SP.
2. Medical devices with the ability to transmit or record data must be approved by the ODFSA.
3. Government owned PEDs, information technology systems may only be authorized for introduction and use within LA's VTR's, PA's and MAA's by the ODFSA. Any ODFSA approval must be based on a documented risk analysis incorporating technical security countermeasures and cybersecurity input.”

*For information or questions about this OES, please contact David Golden (EHSS) at David.Golden@hq.doe.gov or Carrianne Zimmerman (EA) at Carrianne.Zimmerman@hq.doe.gov. For inquiries related to the Operating Experience Program, contact the EHSS Office of ES&H Reporting and Analysis by email at OEC@hq.doe.gov.*

**Operating Experience Summary**

**Operating Experience Summary (OES):** An informative operating experience-based article published by the Office of Environment, Health, Safety, and Security (EHSS) and distributed across the DOE complex through the DOE Corporate Operating Experience Program to promote safety and mission success through the open exchange of valuable experiences, good practices, and performance summaries.

Learn more at: Operating Experience Summaries | Department of Energy