U.S. DEPARTMENT OF ENERGY

EA Enterprise Assessments

2024 DOE Safety and Security Enforcement Workshop

WELCOME BACK!

Anthony Pierpoint
Director
Office of Enforcement
Office of Enterprise Assessments

Agenda

May 8, 2024

8:00 - 8:10	Office of Enforcement Welcome Back	Anthony Pierpoint, Director, Office of Enforcement
8:10 - 8:30	Whistleblower Protection Provisions	Robin Keeler, Deputy Director, Office of Enforcement
8:30 - 9:00	DOE Employee Concerns Program	James Hutton, Director, Employee Workplace Programs Office of Environment, Health, Safety and Security
9:00 - 9:30	Worker Safety and Health Policy News and Update	James Dillard, Director, Office of Worker Safety and Health Policy Office of Environment, Health, Safety and Security
9:30 - 10:00	Break	
10:00 - 10:30	Regulatory Program Assistance Review Discussion	Carrianne Zimmerman, Director, Office of Security Enforcement
10:30 - 11:00	Security Enforcement Presentation - 470.4B Changes	Alan Johnson, IOSC Program Manager, Pacific Northwest National Laboratory
11:00 - 11:45	Phase 1 - Performance Monitoring and Noncompliance Sources	Jason Capriotti, Enforcement Officer, EA-11 Joseph Demers, Enforcement Officer, EA-12 Linwood Livingston, Contractor, EA-13 Heath Garrison, Enforcement Coordinator, NREL

Agenda *(cont'd)*

May 8, 2024

11:45 - 1:15	Lunch	
1:15 - 2:00	Phase 2 - Noncompliance Screening, Identification, and Tracking Systems	Stanley Dutko, Enforcement Officer, EA-11 Christian Palay, Enforcement Officer, EA-12 Karen Sims, Enforcement Officer, EA-13 Tracy Chance, Enforcement Coordinator, Oak Ridge National Laboratory
2:00 - 2:45	Phase 3 - Noncompliance Tracking System and SSIMS Reporting and Closeout	Robert Smith, Enforcement Officer, EA-11 Margaret Kotzalas, Enforcement Officer, EA- 12 Charles Isreal, Enforcement Officer, EA-13 Tamara Baldwin, Enforcement Coordinator, Savannah River Nuclear Solutions
2:45 - 3:15	Break	
3:15 - 4:45	Case Studies | Worker Safety and Health	Room 6339
	Case Studies | Nuclear Safety	Room 6375
	Case Studies | Information Security	Room 6510
4:45 - 5:00	Feedback and Closing	Anthony Pierpoint, *Director, Office of Enforcement*

Whistleblower Protection

Robin Keeler

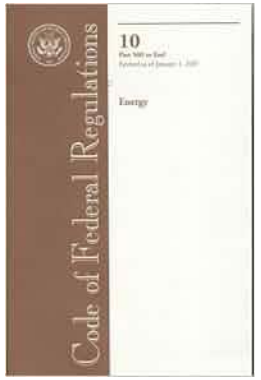
Deputy Director

Office of Worker Safety & Health Enforcement

Office of Enterprise Assessments

Whistleblower Protection

DOE Contractor Employee Protection Program (10 C.F.R. Part 708)



- **Procedures for processing complaints** by employees of DOE contractors alleging retaliation by their employers for disclosure of information **concerning danger to public or worker health or safety, substantial violations of law**, or gross mismanagement; for participation in Congressional proceedings; or for refusal to participate in dangerous activities
- Contractors may file compliant through DOE's Employee Concerns Program (ECP)
- **ECP Officials screen the complaints and forward them to the DOE Office of Hearings and Appeals (OHA)**
- 90-day statute of limitation
- Ruling may be appealed to the Secretary

Whistleblower Protection, cont'd

Energy Reorganization Act (ERA) (42 U.S.C. § 5851 and 29 C.F.R. Part 24)

- Administered by Department of Labor (DOL)
- Applies to Federal and Contractor employees
- Claims processed by an Administrative Law Judge
- **Unlike 708, DOE contractor employees may also file suit in federal court under ERA, after one year**
- **180-day statute of limitation**

Whistleblower Protection, cont'd

Enhanced Whistleblower Protection (41 U.S.C. Section 4712)

- Established as a Pilot Program in 2013 – Expanded scope
- **Investigated by the DOE Inspector General**
- Does not involve formal administrative hearings
- OHA may issue an order of remedy which is enforceable in Federal Court
- **3-year statute of limitation**
- https://www.energy.gov/ig/articles/inspection-report-doe-oig-20-04

Office of Enforcement: Whistleblower Outcomes

1 Enforcement Letter

- **2004**: Westinghouse Savannah River Company at SRS: employee was terminated after raising safety-related issues

3 Preliminary Notice of Violations (PNOVs)

- **2005:** EA-2005-03; 10 CFR 708 violation – Safety and Ecology Corporation at the Portsmouth Gaseous Diffusion Plant for a violation of 10 C.F.R. 708; employee dismissal for raising nuclear safety concerns; Severity Level (SL) 2 violation Civil Penalty = $55,000
- **2008:** NEA-2008-03; 10 CFR 708 violations – Bechtel National, Inc., associated with an employee retaliation for making nuclear safety-related disclosures at the Hanford Waste Treatment and Immobilization Plant (WTP) at the Hanford Site. SL2 CP = $41,250
- **2018:** WEA-2017-02; Savannah River Nuclear Solutions, LLC (SRNS) termination of an SRNS employee at the Savannah River Site. SL1 CP = $320,000 **(10 CFR 851)**

Savannah River Nuclear Solutions

Retaliation Case

Summary

Case involved retaliation by SRNS against the SRNS Employee Concerns Program (ECP) Manager

- Served as the ECP Manager at SRNS for 6 years. Had worked at the site for 37 years
- Fired by SRNS in January 2015
- Case received congressional interest

History and Chronology

August 2014

- U.S. Government Accountability Office (GAO) initiates review of DOE/Contractor Whistleblower Protection Programs; SRNS is included in the review

Fall 2014

- GAO interviews SRNS ECP Manager
- ECP Manager provides documentation following request for information from GAO

January 7, 2015

- SRNS terminates ECP Manager

April 2015

- ECP Manager files a retaliation complaint with DOE's Office of the Inspector General
  - Enhanced Whistleblower Protections (41 USC 4712)
- Also filed complaints under 708 and ERA

History and Chronology, cont'd

January 24, 2017

- **OIG issues Whistleblower Retaliation Investigation Report**
  - Found that the **complainant made a protected disclosure to representatives of the Government Accountability Office** (GAO), and that SRNS management was aware of this disclosure when it terminated complainant's employment on January 7, 2015
  - Further found the **complainant proved that the protected disclosure was a contributing factor in the termination**

S-1 then assigned OHA to adjudicate the finding

History and Chronology

February 23, 2017

- DOE's Office of Hearing and Appeals **(OHA) issues Order to SRNS**
- **OHA orders SRNS to reinstate the employee**. Order includes additional compensatory damages

May 3, 2017

- Office of Enforcement issues Notice of Intent to Investigate to SRNS

History and Chronology, cont'd

August 2017: Enforcement conducted onsite investigation

- Interviewed ECP Manager, ECP Staff and current SRNS President
- Confirmed 10 CFR 851 nexus
  - 3 safety related issues regarding chemical storage, screening, and management, and compressed gas cylinder management
- Evaluated corrective actions

November 8, 2017, in coordination with EM-HQ and DOE-SR, Enforcement issued PNOV to SRNS

- Cites one violation
- Escalation of three additional days for each safety concern
- No mitigation

December 5, 2017, SRNS issues non-contest letter with Civil Penalty payment

Whistleblower Resources

- **DOE's Employee Concerns Program (/ehss/services/doe-employee-concerns-program), or**
- **The DOE Office of Inspector General (/ig/services)**
- **What relief is available to an employee who has suffered retaliation for whistleblowing?**
  - Job restoration
  - Reversal of suspensions and other adverse actions
  - Back pay
  - Reasonable and foreseeable consequential damages, such as medical costs, attorney fees, and compensatory damages
  - In addition, damages may be awarded for attorney fees and expenses incurred due to retaliation

U.S. DEPARTMENT OF ENERGY

EA Enterprise Assessments

Questions?

U.S. Department of Energy
Office of Environment, Health, Safety & Security

Annual Activity Report Fiscal Year 2023

May 2024

Office of Environment, Health, Safety and Security

Annual Activity Report

FY 2023

- DOE O 442.1B, *Department of Energy Employee Concerns Program,* tasks the ECP Director to provide information on program activities, lessons learned, and the effectiveness of DOE and Contractor ECP implementation.

FY 2023 Statistical Data

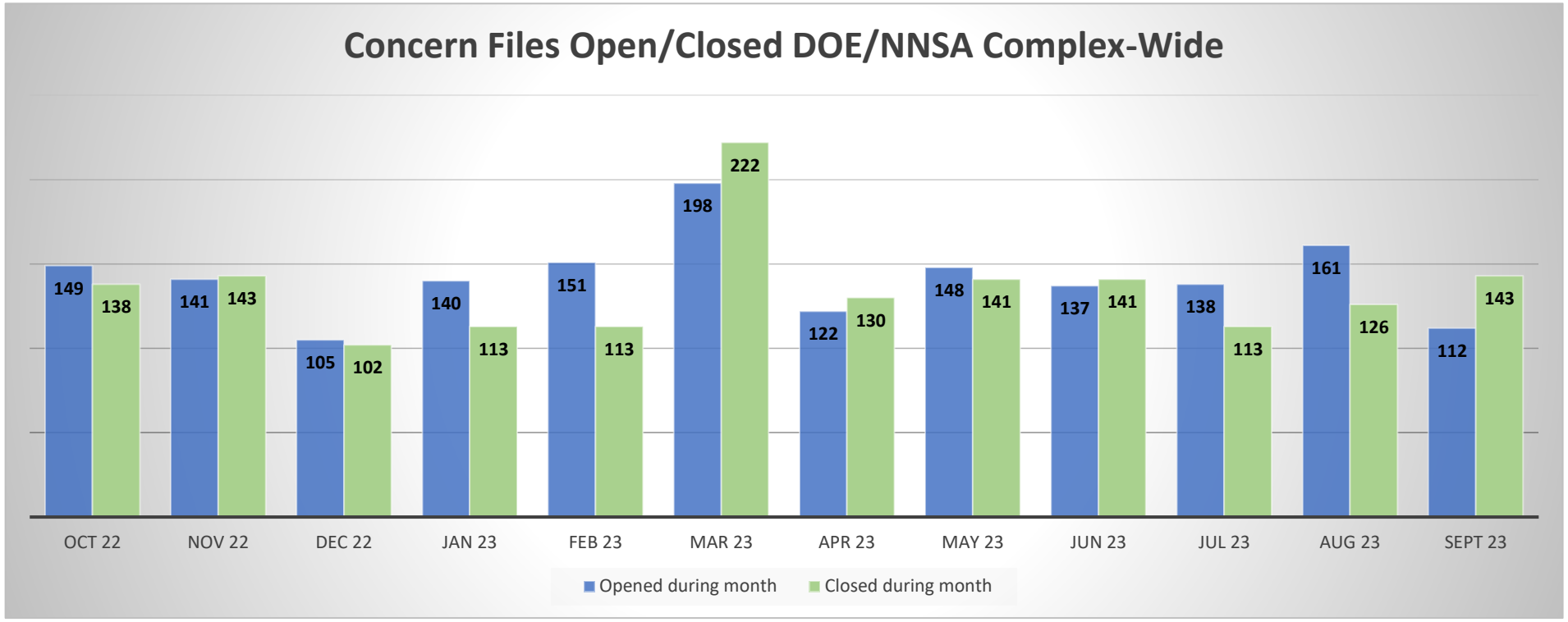
FY23 DOE/NNSA Complex-Wide Activity

Federal ECP Out-of-Scope Contacts	**114**
Federal ECP Concern Files Opened	**188**
Contractor ECP Non-Concern Contacts	**1225**
Contractor ECP Concern Files Opened	**1514**
Total Out-of-Scope Contacts	**1339**
Total Concern Files Opened	**1702**
Total Contacts by Concerned Individuals	**3041**

FY 2023 Statistical Data

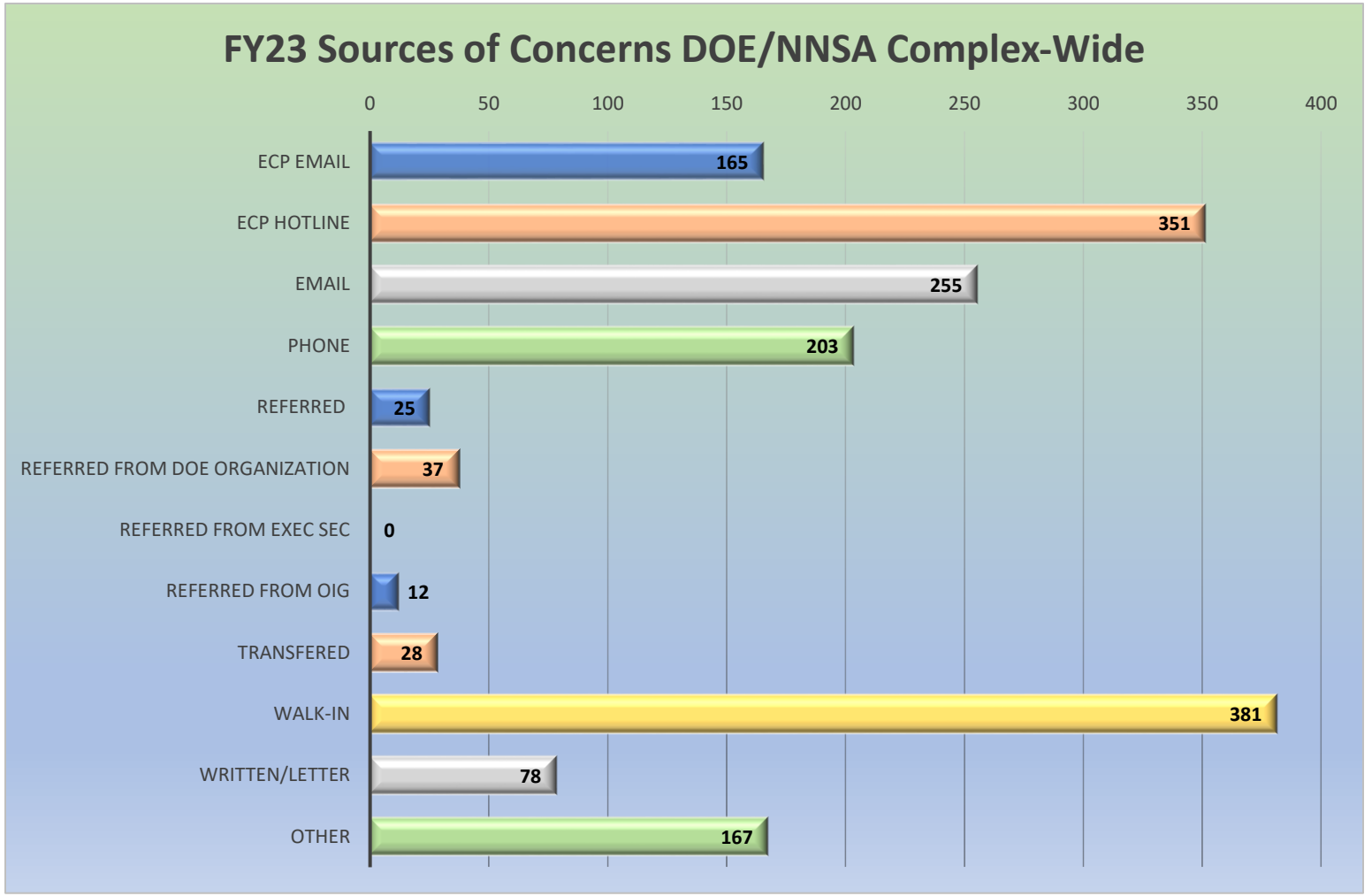
FY23 DOE/NNSA Complex-Wide Activity

	FY22	FY23	
Federal ECP Out-of-Scope Contacts	101	114	+13
Federal ECP Concern Files Opened	280	188	-92
Contractor ECP Non-Concern Contacts	1321	1225	-96
Contractor ECP Concern Files Opened	1558	1514	-44
Total Out-of-Scope Contacts	1422	1339	-83
Total Concern Files Opened	1838	1702	-136
Total Contacts by Concerned Individuals	3260	3041	-219



Monthly Activity

Sources of Concern



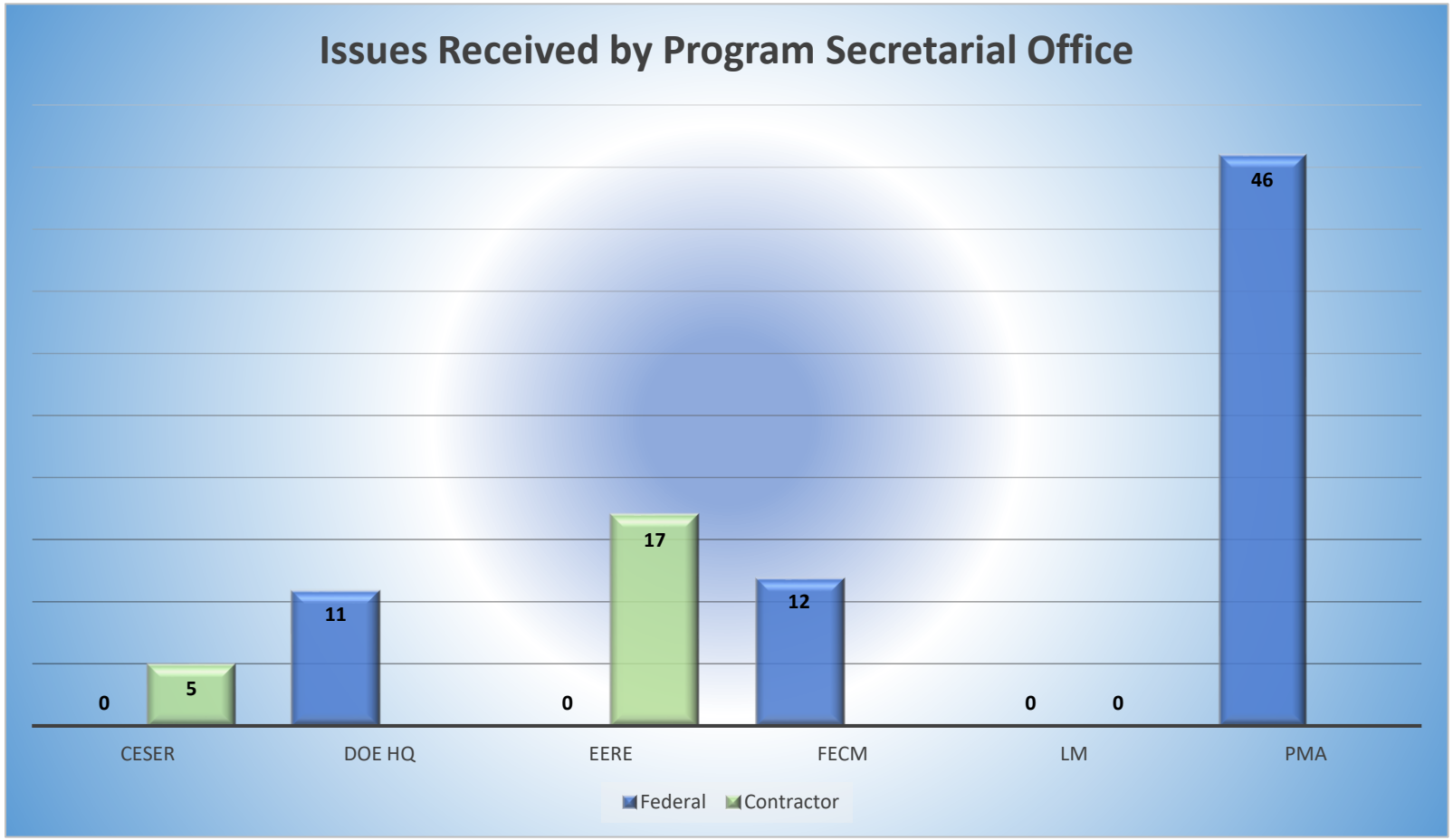
Concern File vs Number of Issues

Each concern will contain at least one Issue and may include several Issues that need to be addressed.

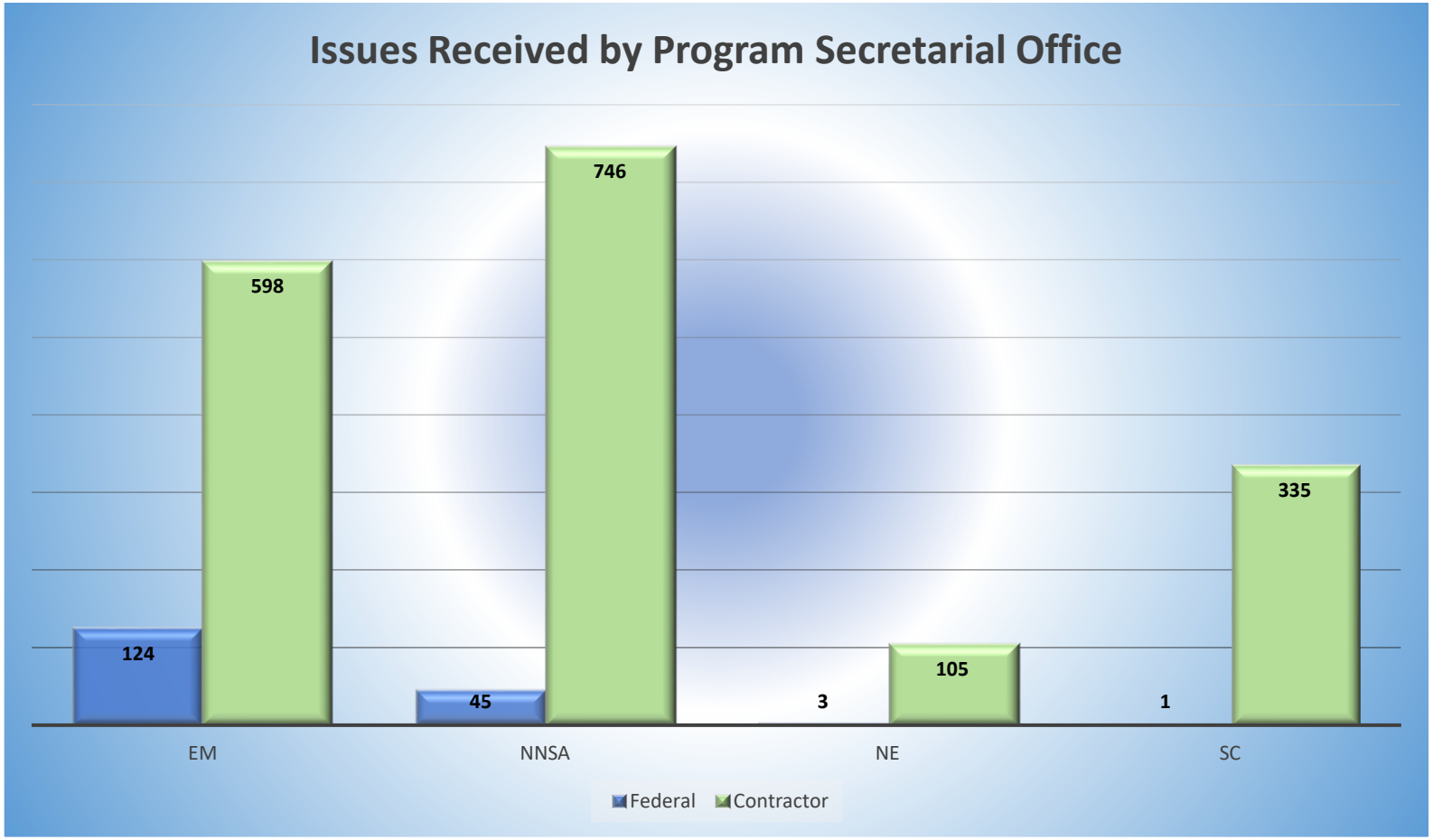
ECPs may process individual Issues separately, as needed, within a concern file, to include transferring any Issues that are outside the scope of the ECP to another organization.

For example, one concern may include a safety Issue, a mismanagement Issue, and an HR Issue within the same concern.

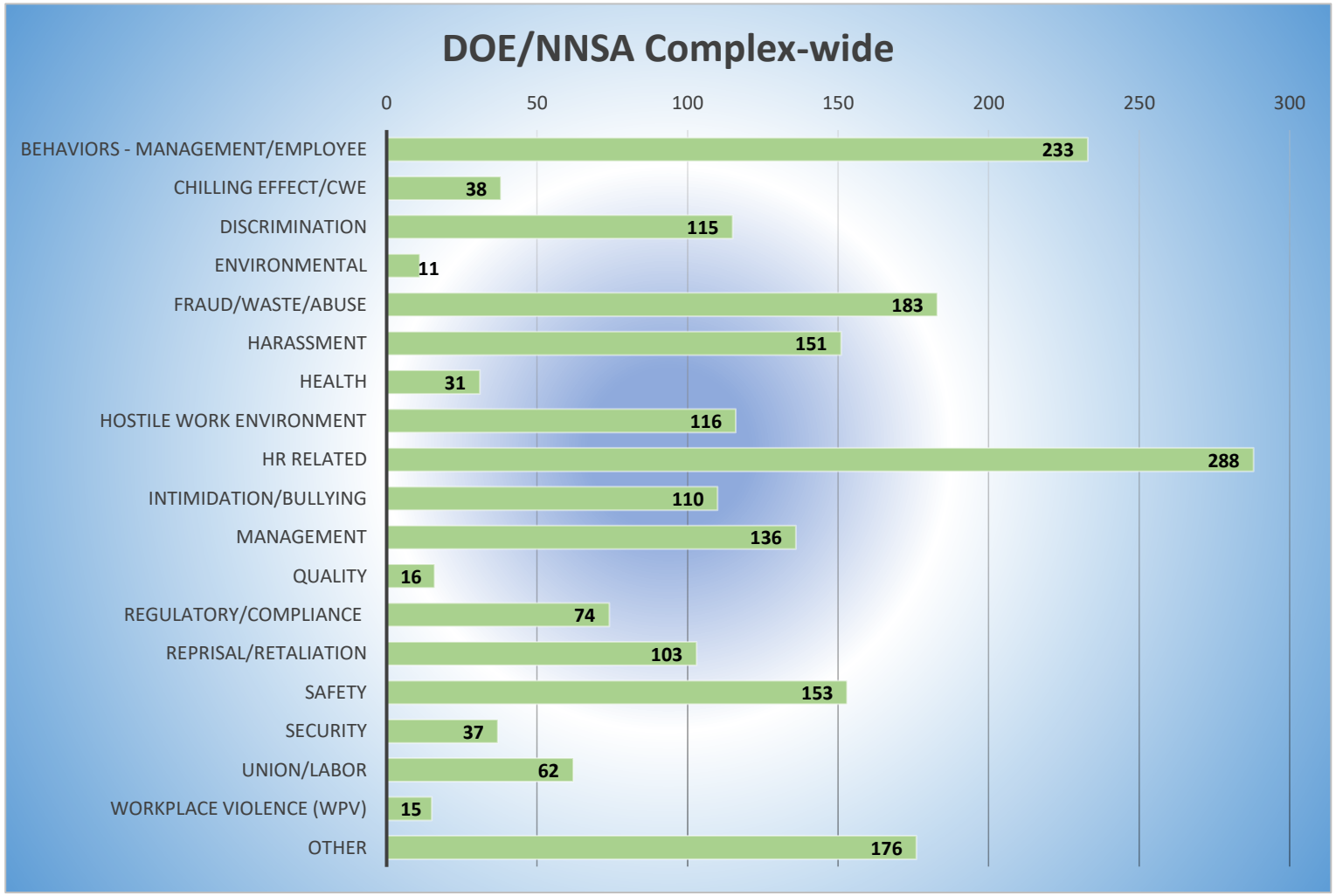
Number of Issues by Program Secretarial Office



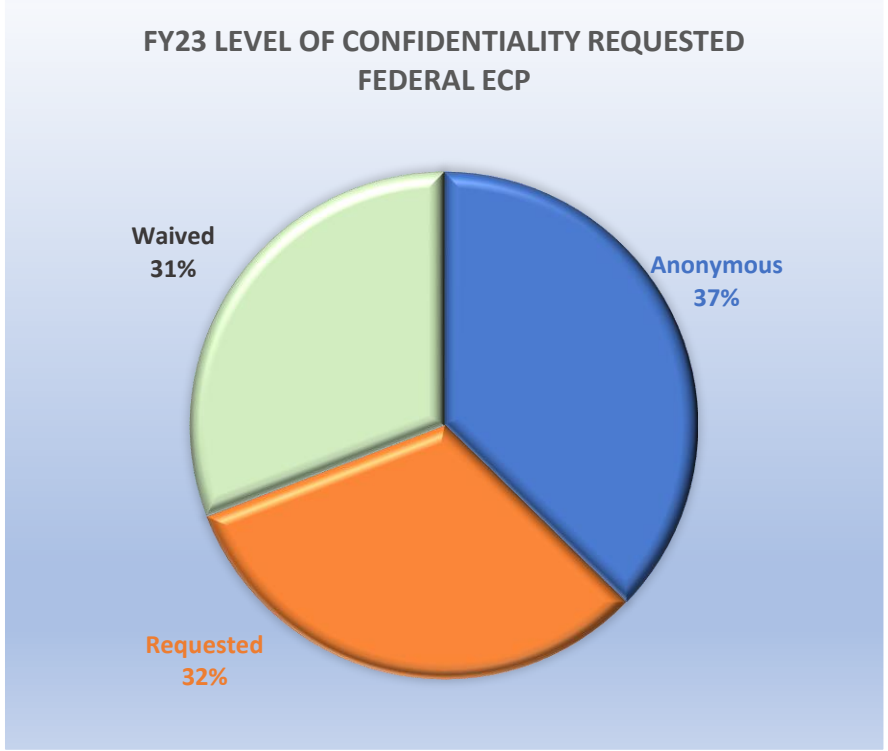
Number of Issues by Program Secretarial Office

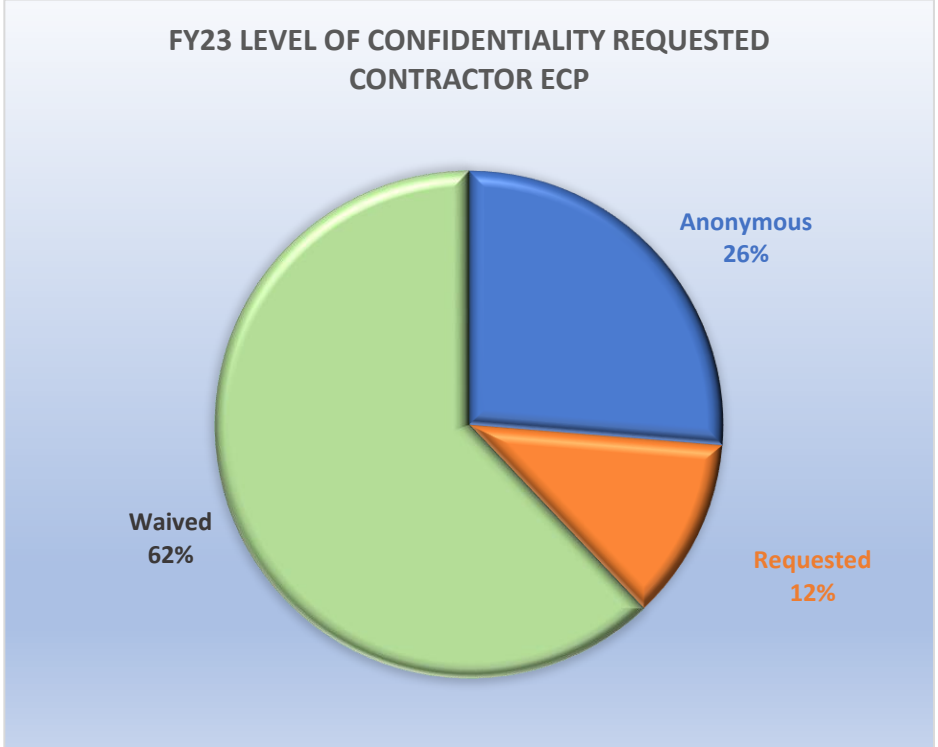


Categories of Issues

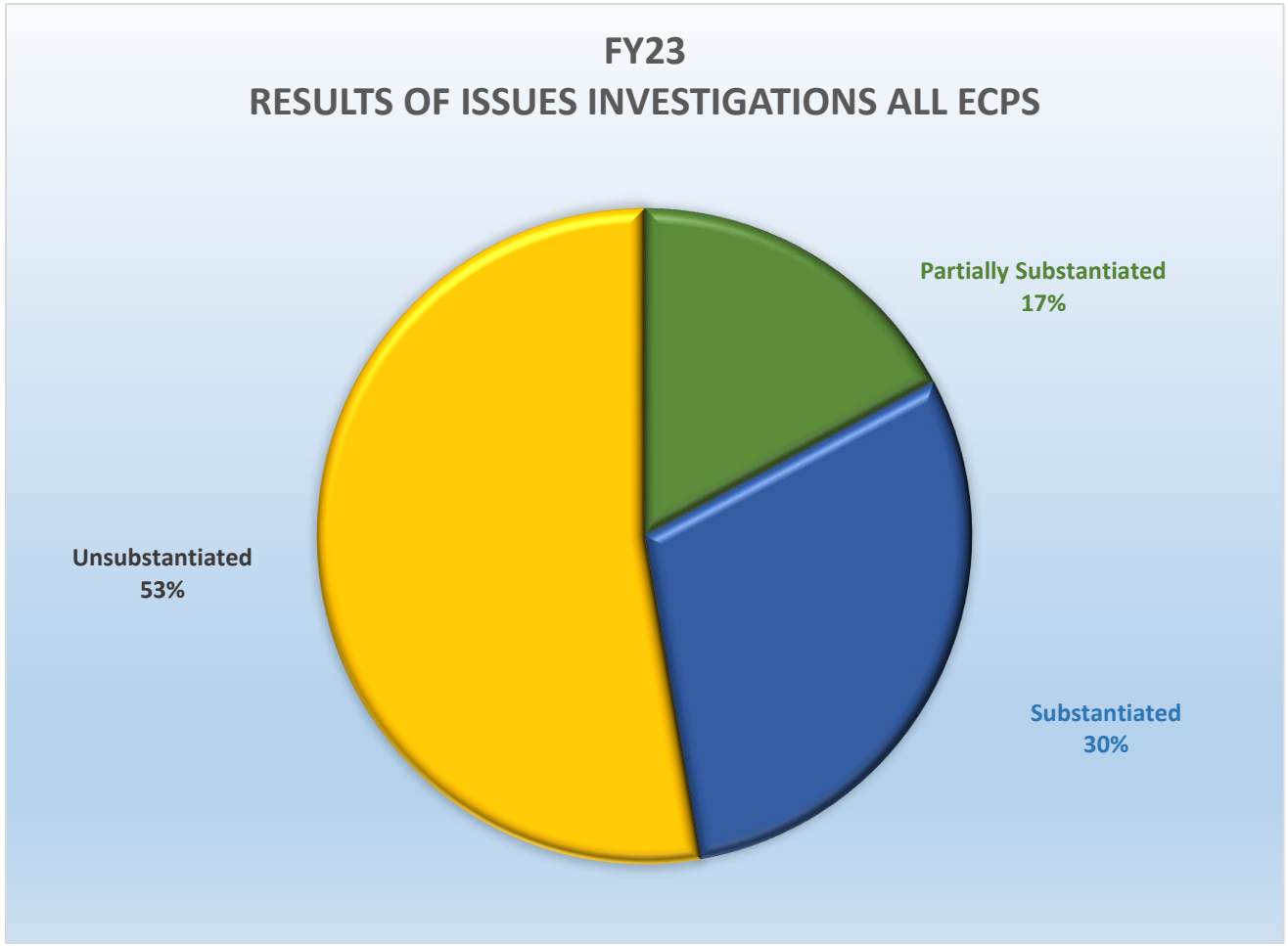


Confidentiality Requested





Disposition of Issues



Program Reviews and Lessons Learned

Program Reviews

- Conducted Program Reviews of 23 DOE/NNSA ECPs
- Included Gap Analysis comparing Site ECP's Procedure to DOE Order
- Evaluated ECPs using *ECP Assessment Objectives and Attributes* document
- Identified Strengths and Areas for Improvement
- Provided recommendations for Program Improvement

Results from Program Reviews

- Site ECPs would benefit from:
  - More definitive ECP procedures
  - Trained/experienced ECP personnel
  - Better communication to site population
  - Stronger senior management support

Lessons Learned

- Clarification of roles/responsibilities
  - Feedback from ECP community
  - Issues identified by OIG Report
  - Issues identified by GAO Report
- Order Revision
- Continuing TLP-310 Training – 2 Classes provided so far

Lessons Learned

- DOE ECP Energy.gov Website:
  https://www.energy.gov/ehss/doe-employee-concerns-program
- Sitewide ECP Contact List:
  https://www.energy.gov/ehss/articles/doe-employee-concerns-program-contact-list
- Annual Notification of Department of Energy's Employee Concerns Program
  https://www.energy.gov/ehss/articles/memorandum-annual-notice-regarding-doe-employees-concerns-program
- DOE ECP Brochure:
  https://www.energy.gov/ehss/articles/ecp-printable-brochure

Office of Worker Safety and Health Policy

Presentation to the 2024 DOE Safety and Security Enforcement Workshop

May 8, 2024

James Dillard, CHP
Director, Office of Worker Safety and Health Policy (EHSS-11)
Office of Environment, Health, Safety and Security
U.S. Department of Energy

Office of Environment, Health, Safety and Security

Environment, Health, Safety and Security

Office of Environment, Health, Safety and Security

Todd Lapointe
Director

Christopher Roscetti
Deputy Director for ES&H

EHSS-1

Office of Health and Safety

Kevin Dressman
Director

EHSS-10

Office of Worker Safety and Health Policy

Jim Dillard
Director

EHSS-11

Worker Safety and Health Policy

Industrial Hygiene

Michael Boley
April Brown
Joe Dobbins
Regina Price
Jackie Rogers (PEC)

Occupational Safety

Moriah Ferullo
Tina Fehringer
Maurice Haygood
Mallory Neyens

Radiation Protection

Dave Pugh
George Chiu

Admin Support

Arlene Schindler-Anim (PEC)

Worker Safety and Health Policy

Establish Departmental expectations for worker safety and health through the development of rules, directives, and guidance.

- Serve as a Federal resource for worker safety and health (WS&H) policy, providing knowledge and support to assist regulated communities in meeting WS&H requirements.
- Identify issues, challenges, and gaps with existing policy structure and work with community recognize available tools and flexibilities and develop new solutions.
- Develop tools to assist DOE programs in implementing and improving WS&H programs.

Responsibilities

- Rulemaking
  - 10 CFR 707, 835, 850, 851
- Policy Support
  - Exemptions/Variances
  - Technical Standards
  - Directives
  - PC Portal
  - FAQs
  - WS&H WebEx
- DOELAP Administration
- FEOSH
  - Program Administration
  - AU Program
- Working Group Support
  - ANSI A10, N13, N43, Z88
  - EFCOG
  - IAEA EGDLE
  - Beryllium Health and Safety
  - Dam Safety Steering Committee

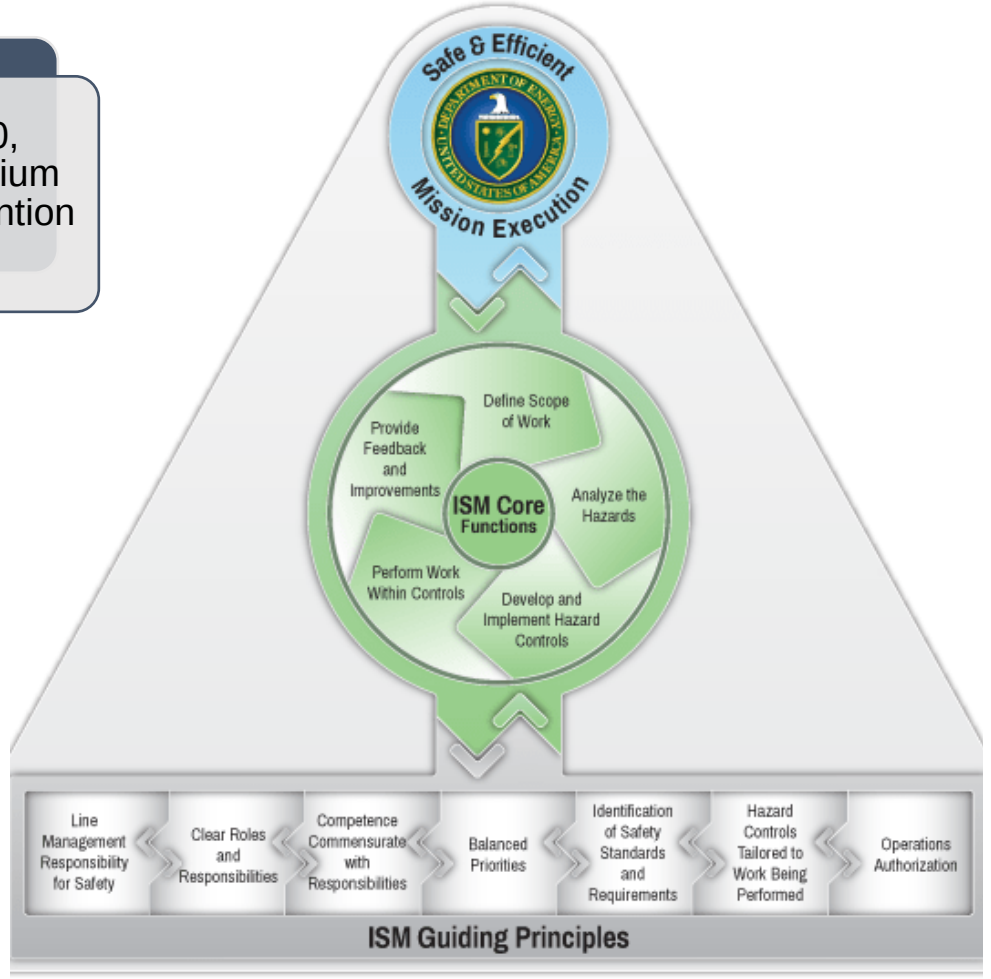
WS&H Framework

10 CFR 851, Worker Safety & Health Program

10 CFR 835, Occupational Radiation Protection

10 CFR 850, Chronic Beryllium Disease Prevention Program

- Prescriptive Requirements
  - Occupational Exposure Limits
  - Contamination Limits
  - Incorporated Standards
- Performance-based requirements
  - Safety and health programs
  - Systematic Approach for preventing hazards
- Implementation Guides
  - DOE G 440.1-1B, 441.101C, 440.1-7A



Policy Initiatives

- Construction Safety
- Integrated Safety Management
  - Benchmarking
  - ISM Champions Counsel
- Laser Safety
  - DOE Laser Exemption
- Pressure Vessels
  - EN Equivalency
- Hard-to-detect radionuclides
- Technical Standards
  - Chemical Safety Management
  - Electrical Safety Program
  - Laser Safety
  - Physiological Monitoring for Heat Strain
  - Radiological Control Technician Training
- Directives
  - Worker Protection Program for DOE

Tools and Resources

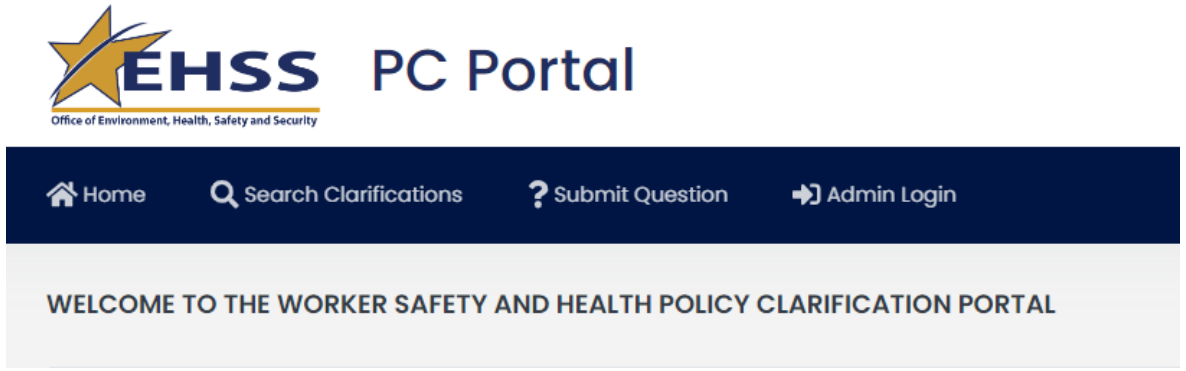
- WS&H WebEx Series

DATE OF WEBEX	TOPIC
Wednesday – May 8	Electrical Safety
Thursday – Jun 20	Rad Protection/Radon
Wednesday – Jul 17	Laser & Fusion Energy
Wednesday – Aug 21	Safety/IH Topic TBD
Wednesday – Sept 18	Accident Investigations
Wednesday – Nov 13	Chemical Safety

- Energy Hub

Tools and Resources

- Policy Clarification Portal
  - Request policy clarification
  - Search clarifications



- WS&H Policy Mailing List

- WebEx invitations
- Policy Clarifications
- Standard/Directive Developments
- Rulemaking news
- Event Notifications

Questions?

Jim Dillard, CHP
Director, Office of Worker Safety and Health Policy
(p)301-903-1165
(e) james.dillard@hq.doe.gov

https://www.energy.gov/ehss/worker-safety-and-health-policy

https://www.energy.gov/ehss/wsh-webex-series-archives
PCPortal.doe.gov

BREAK

9:30 – 10:00

U.S. DEPARTMENT OF ENERGY

EA Enterprise Assessments

Regulatory Program Assistance Review Discussion

Carrianne Zimmerman

Director

Office of Security Enforcement

Safety and Security Regulatory Program Assistance Review – Purpose and Value

- Establish and strengthen communication flow between contractor safety/security/enforcement program personnel and the Office of Enforcement
- Increase senior management awareness of safety and security regulatory program process strengths and challenges
- Offer contractors the opportunity to validate its resource investment in the regulatory program

Safety and Security Regulatory Program Assistance Review – Purpose and Value (cont'd)

- Build confidence in the contractor's ability to effectively identify and correct noncompliance
- Familiarize Office of Enforcement personnel with site operations
- Provide constructive feedback to enhance the safety and security regulatory program processes
- Increase engagement with Federal safety/security/enforcement partners

Safety and Security Regulatory Program Assistance Review – Conduct

- When to recommend a review
  - Never hosted a review
  - New contractor/ new personnel
  - Contractor mission change

Safety and Security Regulatory Program Assessment Review – Conduct (Cont'd)

- Preparation activities
  - Coordinate onsite dates
  - Draft proposed agenda
  - Request documents for pre-onsite visit review

Safety and Security Regulatory Program Assistance Review – Conduct (Cont'd)

- **Pre-onsite visit review activities**
  - Contractor safety and security program plans and procedures
  - NTS and ORPS reports
  - SSIMS Incidents of Security Concern Reports
  - Self-assessment reports
  - Training
  - Issues management

Safety and Security Regulatory Program Assistance Review – Conduct (Cont'd)

- **Post-onsite visit activities**
  - Prepare informal feedback document addressing strengths and recommendations
  - Recommendations are non-mandatory
  - No response required

Safety and Security Regulatory Program Assistance Review – Conduct (Cont'd)

- **Onsite visit activities**
  - 2 – 3 days onsite
  - 2 – 3 Office of Enforcement personnel
  - Interview program management/personnel
  - Review documentation
  - Site familiarization tour
  - Exit meeting

Questions?

Pacific Northwest
NATIONAL LABORATORY

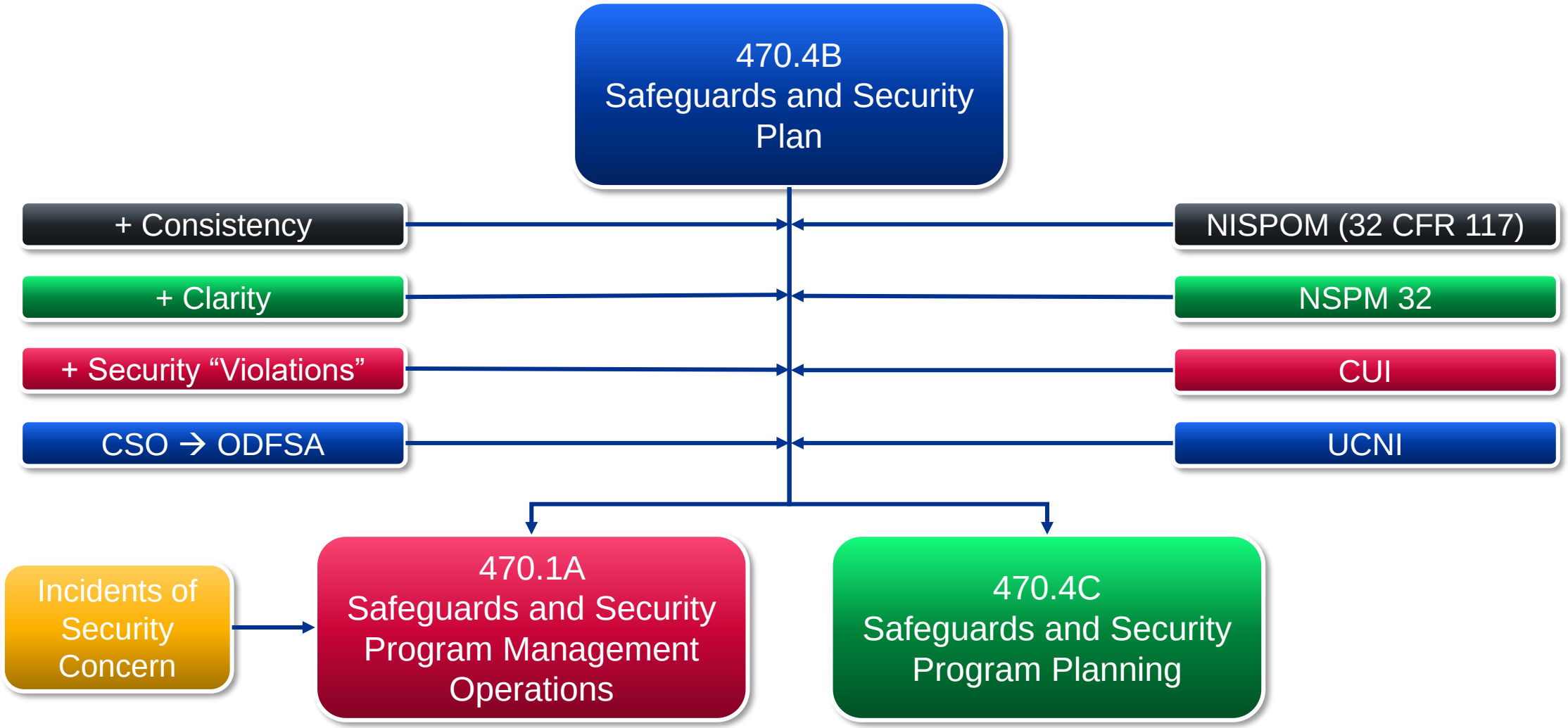
IOSC Changes 470.4B → 470.1A

Alan Johnson
IOSC Program Manager, PNNL

U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

Background


470.4B
Safeguards and Security Plan
+ Consistency
+ Clarity
+ Security "Violations"
CSO → ODFSA
NISPOM (32 CFR 117)
NSPM 32
CUI
UCNI
Incidents of Security Concern
470.1A
Safeguards and Security Program Management Operations
470.4C
Safeguards and Security Program Planning

Process (So Far…)

- Identify broad group of stakeholders
- Solicit “wish list”
- Pare wish list down through group consensus and continuous feedback cycle
- Pre-RevCom feedback on proposed changes
- RevCom comment resolution (and late comment resolution)

Not Included…

All IOSCs in SSIMS

Unclassified database for ALL IOSCs

Cat A Closure beyond 90 days

Limit IOSCs to SNM and classified

Full NSPM-32 reporting burden

Make ALL IOSCs the same across Complex (no local oversight input)

Leave ALL IOSCs under local oversight input (no consistency)

Significant Changes

Lost/stolen badge ≠ IOSC	When IOSCs are "closed"	5 Calendar Days → Business Days	Improved IOSC Category and Type definitions	Expanded baseline list of reportable events
Improved definitions for types of compromise	Defined culpability and intent for consistent usage	Consolidated IOSC Program Plan requirements	Security Infractions AND Violations	Roles for Inquiry Officials in training
Eliminate/reduce redundant reporting streams (ORPS, Cyber)	CUI "misuse"	CPSO Reporting for ALL IOSCs	Special Reporting Situations	Sanitization → CIO

Challenges


NSPM 32
Timeline Exceptions
SSIMS
Standard Retirement
Balance Local Oversight and Complex Consistency
Sync DOE/NNSA Requirements
Culpability Reporting and Administrative Actions
Stakeholder Identification and Engagement
CUI vs. UCNI
ISC

Snapshot: Cat A vs Cat B

Cat A IOSC

- Those IOSCs which have a significant detrimental impact on DOE or national security, often because of the loss, theft, compromise, or potential compromise of a *significant* security asset (e.g., classified matter, SNM). As such, they require the notification and involvement of the Officially Designated Federal Security Authority (ODFSA) and Officially Designated Security Authority (ODSA) (where applicable). Category A IOSCs must also be reported and documented in the Safeguards and Security Information Management System (SSIMS). Category A IOSCs also require a higher level of effort and detail (i.e., graded response) to significantly reduce the likelihood of recurrence (e.g., cause analysis, corrective action plan, extent of condition).

Cat B IOSC

- Those IOSCs which have a less significant detrimental impact on DOE or national security. These IOSCs typically *do not involve* the loss, theft, compromise, or potential compromise of *significant* security assets, but if uncorrected they reasonably could. Category B IOSCs *may involve* the loss, theft, compromise, or potential compromise of *less significant security assets* (e.g., Controlled Unclassified Information [CUI]). Oversight responsibilities for Category B IOSCs remain with the ODFSA; however, Category B IOSCs are managed and resolved by the ODSA (or equivalent ODFSA designee). Category B IOSCs must be reported either in SSIMS or in a local tracking system as specified in the IOSC Program Plan. When reporting a Category B IOSC, the lower significance must be justified (i.e., loss, theft, compromise, or potential compromise did not occur or is remote). In addition, a lower graded response is typically appropriate.

Snapshot: Compromise Types

Compromise

- A final determination that classified information or Unclassified Controlled Nuclear Information (UCNI) is/was disclosed to one or more unauthorized individuals, or the information was outside of appropriate controls and cannot subsequently be placed back under appropriate controls (e.g., published by media, UCNI or classified information was provided to unauthorized individuals). Compromises of classified information are reported as Category A SI IOSCs.

Potential Compromise

- At the conclusion of an inquiry into a suspected compromise, there may be inadequate evidence to determine whether a (actual) compromise occurred, did not occur, or whether the likelihood of compromise is remote. In this case, the inquiry will make the final determination that a potential compromise occurred. Although there is no clear indication or evidence of compromise (e.g., no direct recipient), the circumstances associated with the IOSC indicate that there is an obvious possibility that unauthorized disclosure occurred, and compromise is not remote. The IOSC will be treated as a compromise even though there is no definitive evidence that a compromise occurred. (A final determination that a potential compromise of classified matter occurred must be reported as a Category A IOSC.)

Likelihood of Compromise Is Remote

- An inquiry may determine that the likelihood of compromise is remote. For this (final) determination, although protection and control measures are violated, the circumstances associated with the IOSC indicate that there is a low possibility that information was disclosed to unauthorized personnel. Noncompliances involving classified information where the likelihood of compromised is determined to be remote are typically reported as Category B PI IOSCs. Examples include, but are not limited to:
  - Classified information is left unsecured and unattended for a limited amount of time in an area accessed only by appropriately cleared individuals.
  - Classified information is discovered on an unauthorized government- furnished computer system or network, but metadata confirms it was only accessed by appropriately cleared individuals.
  - Unmarked encrypted classified information is transmitted to only cleared recipients on a government-furnished computer system/network not approved for classified information.

Compromise Did Not Occur

- A final determination that there is no possibility of compromise. Noncompliances involving classified information where compromise did not occur are typically reported as Category B PI IOSCs.

Snapshot: Security Violations vs. Infractions

Security Infraction

- Security infractions are documented and reported to the Cognizant Personnel Security Office (CPSO) using DOE F 5639.3 or equivalent as documented in the IOSC Program Plan. Infractions are both a method for characterizing a noncompliance that did not result in a (security) violation (i.e., loss, theft, compromise or potential compromise did not occur), as well as formal documentation (i.e., an administrative action) issued to a person or persons under the following circumstances:
  - Classified information was mishandled; or
  - UCNI was mishandled; or
  - "Misuse" of CUI-specified.
- Note: the issuance of a security infraction will only be associated with Category B IOSCs, versus security violations which are issued for Category A IOSCs.

Security Violation

- Security violations are documented and reported to the CPSO using DOE F 5639.3 or equivalent as documented in the IOSC Program Plan. Security violations are both a method for characterizing a noncompliance (e.g., a violation of policies or requirements) as well as formal documentation (i.e., an administrative action) issued to a person or persons under the following circumstances:
  - The IOSC resulted in the loss, theft, compromise or potential compromise of classified or UCNI; or
  - The IOSC did not result in the loss, theft, compromise or potential compromise but reasonably could be expected to and is the result of gross negligence or a willful act; or
  - Any knowing, willful, or grossly negligent action to classify or continue the classification of information contrary to federal requirements; or
  - Any knowing, willful, or negligent action to create or continue a special access program contrary to federal requirements; or
  - The IOSC is reported as a Category A SI and one or more responsible persons are identified.

Snapshot: Culpability

Inadvertent

- An action or inaction contrary to requirements or procedures where neither the act (or omission) nor the outcome were deliberate or intended. Generally, the result of temporary (vs. habitual) inattention while the individual is making a good faith effort to follow prescribed procedures as they understand them.

Negligence

- An action, inaction, or omission, contrary to requirements or procedures (i.e., noncompliance) that fails to display a reasonable degree of care and attention under the circumstances. The noncompliance could reasonably be expected to result in the loss or compromise of DOE security assets. The noncompliance may be the result of a knowing circumvention of requirements or procedures, but with a good faith expectation of an overriding positive outcome. If loss or compromise of classified information or UCNI does occur, results in a security violation. If loss or compromise does not occur or if CUI is “misused”, typically results in a security infraction for the responsible individual(s). Note: a noncompliance may be unintentional (the responsible individual did not intend the noncompliant outcome) yet still negligent because the individual did not make a good faith effort to follow prescribed procedures.

Gross Negligence

- An action or inaction contrary to requirements or procedures which demonstrates such inattention and carelessness as to appear reckless or intentional. A reasonable person would recognize that the act (or omission) has a high probability of resulting in the loss or compromise of DOE security assets. For example, a person may circumvent prescribed procedures with full knowledge of the security requirements and associated penalties but does so for personal convenience with little concern for the compromise or potential compromise of the security asset. Gross negligence also includes acts (or omissions) which are not deliberate in nature but reflect a recent or recurring pattern of questionable judgement, irresponsibility, negligence, or carelessness. Results in the issuance of a security violation for the responsible individual(s).

Willful

- A willful noncompliance refers to a determination that an employee deliberately disregarded (i.e., ignored), intentionally violated, or was aware of a violation of, a security requirement and, in addition, the employee either attempted to conceal the violation or made no reasonable attempt to eliminate or abate the conditions that gave rise to the violation. Willful noncompliances must be reported through the SSIMS. Results in the issuance of a security violation for the responsible individual(s).

Snapshot: “Misuse” of CUI

Misuse of CUI occurs when someone uses CUI in a manner not in accordance with the policy contained in DOE O 471.7 (or successor policies), 32 CFR Part 2002, the CUI Registry, agency CUI policy, or the applicable laws, regulations, and government-wide policies that govern the affected information. Misuse includes, but is not limited to:

CUI-Specified information (e.g., UCNI, CUI//SP-NNPI, CUI//SP-EXPT) from a document or matter appropriately marked as CUI-Specified (i.e., an excerpt) is intentionally released to someone who does not have lawful government purpose (LGP) requiring access to the information to perform their duties or other DOE-authorized activities.

Intentionally OR negligently releasing a CUI-Specified-marked document (or matter), in its entirety, to someone who does not have an LGP.

Snapshot: Category A Security Interest IOSCs

- Loss, theft, diversion, or unauthorized access to (e.g., compromise of) accountable quantities of Category I or II SNM or other nuclear material controlled and accounted for as SNM …
- Loss, theft, or diversion of accountable quantities of Category III or IV SNM or other nuclear material controlled and accounted for as SNM …
- Loss, theft, compromise, or potential compromise of classified matter;
- Unauthorized disclosure of Sigma 14 or 20 Nuclear Weapon Data (NWD) to a Q-cleared person …
- Loss, theft, or unauthorized access to (e.g., compromise of) a quantity of radiological, chemical, and/or biological materials …
- Loss or theft of security key, keycard, or badge (e.g., DOE PIV) which provides unimpeded access to SNM or classified matter …
- Loss, theft, or other inventory shortages of DOE firearms, explosives …
- Loss, theft, compromise, or potential compromise of foreign government material or information …
- Loss, theft, compromise, or potential compromise of other assets determined by the ODFSA and/or ODSA …

Snapshot: Category B Security Interest IOSCs

Confirmed theft or diversion with malicious intent (e.g., attempted theft) of OANM …

Unauthorized disclosure of Sigma 15 Nuclear Weapon Data (NWD) to a Q-cleared person which would not be otherwise approved …

Loss, theft, or compromise of UCNI;

Intentional or negligent "misuse" of CUI-Specified …

Other assets as determined by the ODFSA and/or ODSA and documented in the IOSC Program Plan

Snapshot: Category A Procedural Interest IOSCs

Any unauthorized discharge of a firearm, pyrotechnic, or explosive …

Any knowing, willful, or grossly negligent action to classify or continue the classification of information contrary to federal requirements;

Any knowing, willful, or negligent action to create or continue a special access program contrary to federal requirements;

Willful noncompliances (i.e., deliberate violations) with requirements for the protection of classified information (which do not result in loss, compromise, or potential compromise); or

Other events as determined by the ODFSA and/or ODSA and documented in the IOSC Program Plan.

Snapshot: Category B Procedural Interest IOSCs

The improper handling, and/or storage of classified matter.

The improper processing or transmission of classified matter on unauthorized computer systems/networks (e.g., encrypted unmarked classified information transmitted to only cleared personnel on government-furnished equipment, applications, or networks not authorized to process classified).

An unsecured door (or other boundary) for a security area authorized for the storage, access, or processing of classified matter or SNM.

Unauthorized access (e.g., circumvention of access control requirements/controls) into a security area authorized for the storage of classified matter or SNM.

Any negligent action that results in the misclassification of information. (Misclassification that results in compromise will be handled in accordance with applicable SI reporting requirements.)

Intrusion Detection System (IDS) failure without appropriate Protective Force response or implementation of other authorized compensatory measures (where IDS is required).

Diversion of accountable quantities of Cat III or IV SNM or any other circumstance resulting in Cat III or IV SNM … in an unauthorized (but Federally controlled) location (if there are no indications of malicious intent).

Failure to obtain appropriate approvals for Foreign National access to DOE facilities, information, technologies or equipment (that is not administratively corrected after the fact).

Improper issuance or termination of a DOE security credential (i.e., Personal Identity Verification [PIV] badge).

Any unapproved controlled article which poses a threat to classified matter (e.g., a controlled article in close proximity to classified discussions, matter, or processing) …

Other events as determined by the ODFSA and/or ODSA and documented in the IOSC Program Plan.

Pacific Northwest
NATIONAL LABORATORY

Thank you

Questions/Comments?
Contact IPT IOSC Sub-Working Group Leads:
Alan.Johnson@pnnl.gov
grselig@sandia.gov
(Greg Seligman)

Phase 1- Performance Monitoring and Noncompliance Sources

Jason Capriotti
Enforcement Officer
Office of Worker Safety and Health Enforcement

Joseph Demers
Enforcement Officer
Office of Nuclear Safety Enforcement

Liv Livingston
Unwin
Office of Security Enforcement

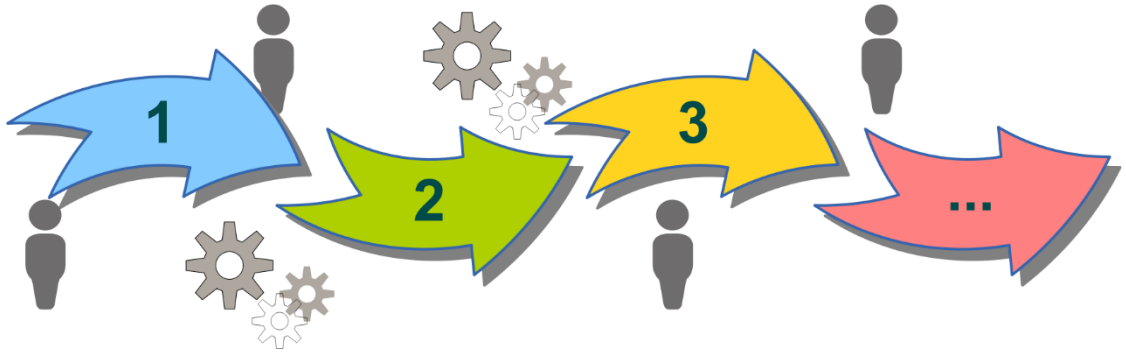
Heath Garrison
Enforcement Coordinator
National Renewable Energy Laboratory

Safety and Security Regulatory Compliance Program Process

Phase 1: **PERFORMANCE MONITORING AND NONCOMPLIANCE SOURCES**

Phase 2: Noncompliance Screening, Identification, and Tracking Systems

Phase 3: Noncompliance Tracking System and SSIMS Reporting and Closeout

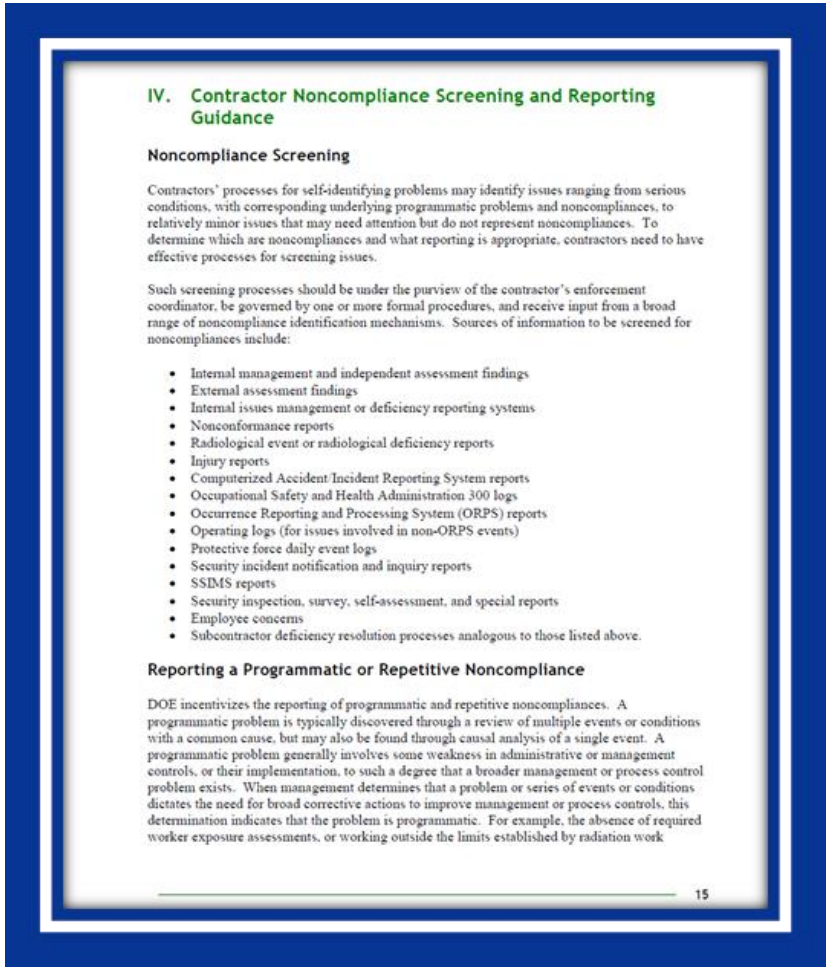


FOR DISCUSSION……

- Performance Monitoring & Compliance Assurance
- Methods and Approaches to identification
- Evaluating performance data for repetition or programmatic failure

Performance Monitoring & Compliance Assurance Information Sources

- Event reporting
  - Occurrence Reports
  - Incidents of Security Concern
- Assessment Results
  - External Assessments
  - Internal Contractor Assessments
- DNFSB reports
- Site/Field Office reports and meetings
- CAIRS (Injury and Illness Reports)
- Nonconformance Reports
- Performance Metrics
- Equipment Performance Data
- Trend Analysis
- Management Walk Around
- Inspections



IV. Contractor Noncompliance Screening and Reporting Guidance

Noncompliance Screening

Contractors' processes for self-identifying problems may identify issues ranging from serious conditions, with corresponding underlying programmatic problems and noncompliances, to relatively minor issues that may need attention but do not represent noncompliances. To determine which are noncompliances and what reporting is appropriate, contractors need to have effective processes for screening issues.

Such screening processes should be under the purview of the contractor's enforcement coordinator, be governed by one or more formal procedures, and receive input from a broad range of noncompliance identification mechanisms. Sources of information to be screened for noncompliances include:

- Internal management and independent assessment findings
- External assessment findings
- Internal issues management or deficiency reporting systems
- Nonconformance reports
- Radiological event or radiological deficiency reports
- Injury reports
- Computerized Accident/Incident Reporting System reports
- Occupational Safety and Health Administration 300 logs
- Occurrence Reporting and Processing System (ORPS) reports
- Operating logs (for issues involved in non-ORPS events)
- Protective force daily event logs
- Security incident notification and inquiry reports
- SSIMS reports
- Security inspection, survey, self-assessment, and special reports
- Employee concerns
- Subcontractor deficiency resolution processes analogous to those listed above.

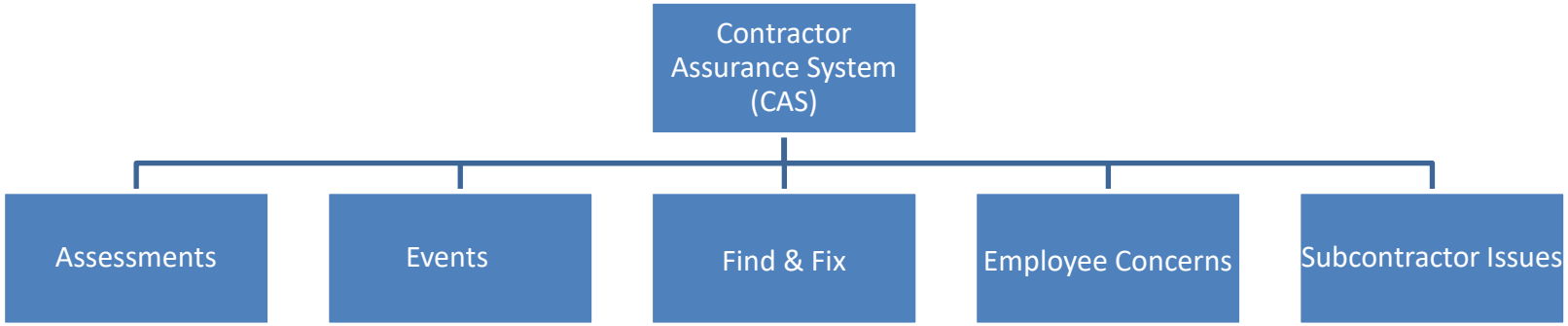
Reporting a Programmatic or Repetitive Noncompliance

DOE incentivizes the reporting of programmatic and repetitive noncompliances. A programmatic problem is typically discovered through a review of multiple events or conditions with a common cause, but may also be found through causal analysis of a single event. A programmatic problem generally involves some weakness in administrative or management controls, or their implementation, to such a degree that a broader management or process control problem exists. When management determines that a problem or series of events or conditions dictates the need for broad corrective actions to improve management or process controls, this determination indicates that the problem is programmatic. For example, the absence of required worker exposure assessments, or working outside the limits established by radiation work

15

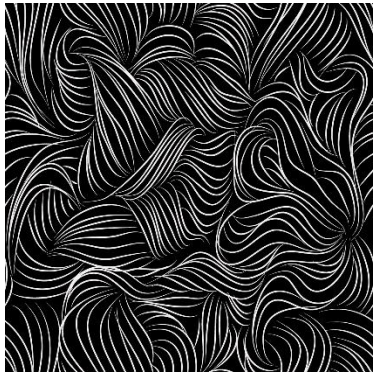
*Found on **Page 15** in Safety/Security Enforcement Coordinator Handbook

Methods and Approaches



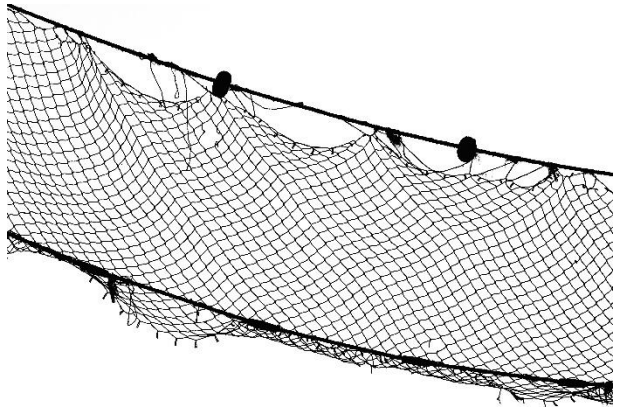
Data Evaluation & Trend Analysis

Look for Patterns, Trends, and Low-Level Events that may be a precursor to a high significance consequence.



Do ***NOT*** limit your sources of information for identifying potential non compliances.

-Cast a wide net!-



The objective of the enforceable rules is prevention, so be proactive not reactive.

U.S. DEPARTMENT OF ENERGY

EA Enterprise Assessments

Questions?

Thank You for Participating!

LUNCH

11:45 – 1:15

Phase 2- Noncompliance Screening, Identification, and Tracking Systems

Stanley Dutko
Enforcement Officer
Office of Worker Safety and Health Enforcement

Christian Palay
Enforcement Officer
Office of Nuclear Safety Enforcement

Karen Sims
Enforcement Officer
Office of Security Enforcement

Tracy Chance
Enforcement Coordinator
Oak Ridge National Laboratory

Expectations for Identification of Noncompliances

- Monitor performance and identify events, conditions, and issues that may reveal noncompliances
- Contractor identification is the preferred means as it promotes earlier prevention of problems affecting safety and security
- Reactive detection is also important (e.g., external, self-disclosing events, extent of condition reviews)

Expectations for Screening

- Record, evaluate, and correct all noncompliances
- Engage subject matter experts in identifying appropriate noncompliances
- Determine who performs screening
- Office of Enforcement regulatory program assistance reviews (RPARs) are available upon request

EA-11 Sources of Noncompliance

- **Enforcement Officers review the following Sources of Noncompliances and recommend if enforcement action is warranted for an event or condition:**
  - ORPS, CAIRS & NTS report(s)
  - DOE HQ or field inspections / Surveys or assessment
  - Inspector General report(s) / Defense Nuclear Facilities Safety Board report(s)
  - Information from other agencies such as OSHA
  - Allegations communicated directly to Office of Enforcement
- **Contact EA-12 and EA-13 Enforcement Officer(s) to discuss any regulatory overlap between Worker Safety, Nuclear Safety and Security**

Common Screening Weaknesses

- Not evaluating all sources of potential noncompliances
- Use of overly limiting screening criteria
- Failure to consider all applicable standards
- Justifications for not identifying noncompliances
- Category B information security events vs Category A
- Repetitive event or condition or programmatic issue not identified

EA-12 Sources of Noncompliances

- **Nuclear Safety Enforcement Officers review the following to determine if enforcement action is warranted:**
  - ORPS & NTS reports
  - DOE HQ or Field/Site Office assessment reports
  - Information from other DOE entities such as IG, OHA, EA-30
  - Defense Nuclear Facilities Safety Board correspondence and staff report(s)
  - Requests for Investigation submitted directly to the Office of Enforcement
  - Media reports
- **Nuclear Safety Enforcement Officers coordinate with the other Enforcement Officer(s) to discuss any regulatory overlap between Worker Safety, Nuclear Safety, and Security**

EA-13 Sources of Noncompliances

- **Information Security Enforcement Officers review the following to determine if enforcement action is warranted:**
  - **Security incident reporting per DOE Order 470.4B, Chg. 2:**
    - Inquiry/Investigation conducted discloses violation(s) of classified information security requirements
    - Safeguards and Security Information Management System (SSIMS)
  - **Findings or issues identified during assessments/appraisals:**
    - Security and cyber assessments
    - HQ or local security surveys
    - IG or GAO reports
    - Requests for Investigation

EA-13 Security Significance Screening

Incident Number	Sample SSDW	Local Tracking Number	XXX-YYYY	Categorization	A	IP/SI
Cognizant Security Office	Program Secretarial Office	Facility Name	Company Name		SSIMS IOSC Status	
XXX	XXX	XXX	XXXXXXX		☑ Notification	☑ Closed

Dates				IOSC Description	Brief Description
Discovery	Notification	Inquiry Report	Closed (SSIMS)		
4/1/2023	4/15/2023	8/28/2023	8/29/2023		

Classification Level	Significance Weight	Category	Significance Weight	Caveat	Significance Weight	Disclosure Determination	Site Sig Wt.	Enf Sig Wt.	Non-Compliance Characterization	Site Sig Wt.	Enf Sig Wt.	Contributing Factors	Significance Weight
TS		RD		SAP		Loss Did Occur			Willful			Management Involvement	
S		FRD		SCI		Loss is Not Remote			Gross Negligence			FN Sensitive Country	
C		NSI		NWD - Sigmas		Loss is Remote			Negligence			FN Non-Sensitive Country	
UCNI		TFNI		All Other NWD		Loss Did Not Occur			Inadvertent			Identified by External Source	
				All Other Caveats								Other Contributing Factors	
				None								None	
Subtotal	0	Subtotal	0	Subtotal	0	Subtotal		0	Subtotal		0	Subtotal	0

Incident Notification Significance Value	0	Final Incident Significance Value		*See Significance Keys at the bottom of the Worksheet.*

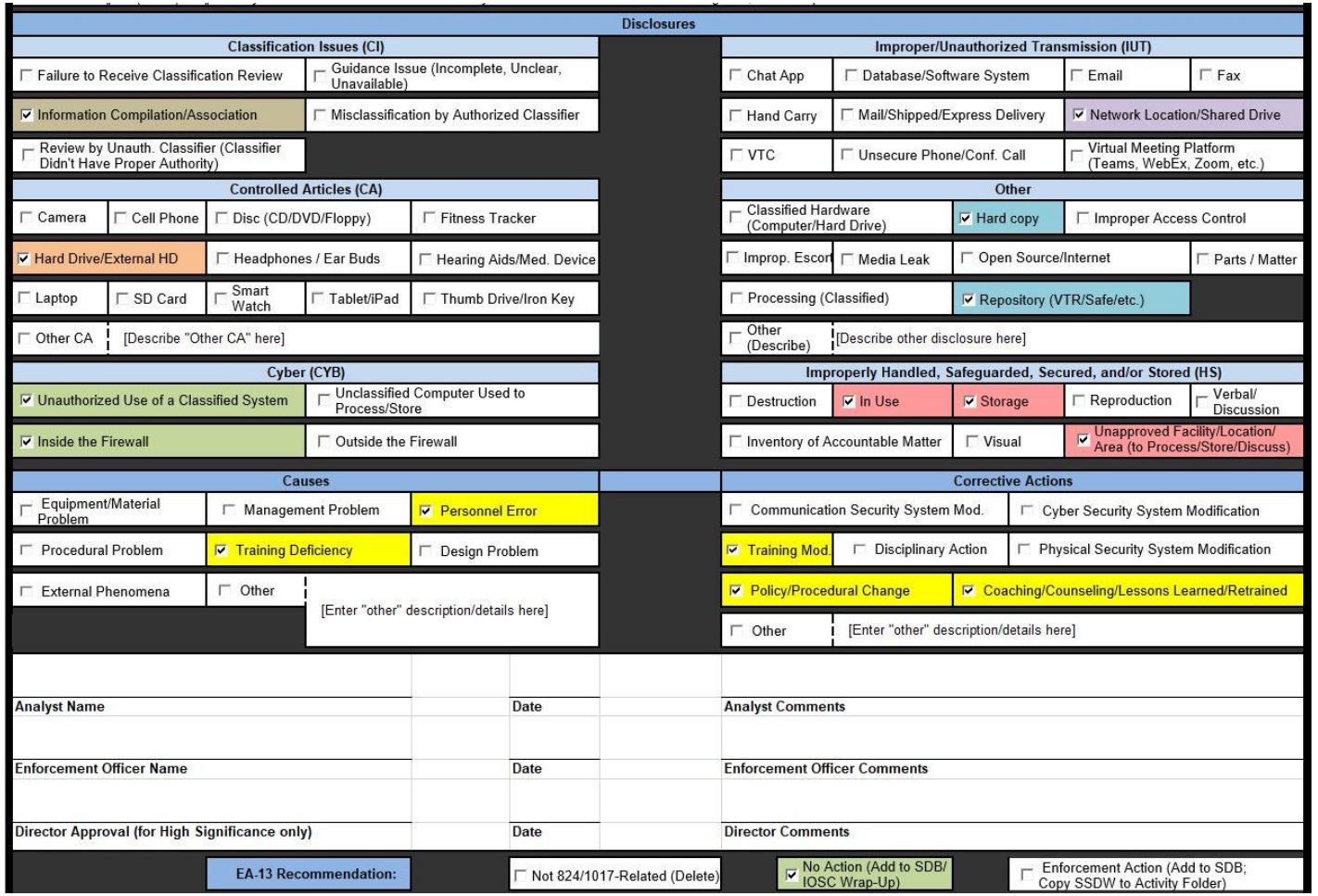
Light Grey Shade Area/Fields = Incident Notification Fields; White Area/Fields = Additional Fields Completed After IR Review

All Other Caveats Description:	CAVEAT

Incident Notification Significance Determination Key		
≥ 15	High (Red)	Security incident of the highest order that almost always needs closer review upon completion of the inquiry by the responsible facilities inquiry officer. These incident notifications should be flagged for follow-up and discussed with the Director, Office of Security Enforcement.
11-14	Serious (Yellow)	Closer review on the circumstances and extent of non-compliance should be undertaken upon completion of the inquiry by the responsible facilities inquiry officer.
7-10	Marginal (Green)	These incidents should be evaluated with contributing factors upon completion of the inquiry by the responsible facilities inquiry officer. In some cases, a closer review may be necessary.
1-6	Low (White)	These incidents should be evaluated with contributing factors upon completion of the inquiry by the responsible facilities inquiry officer. These may not result in a closer review.

Final Incident Significance Determination Key		
>28	High (Red)	Enforcement problem of the highest order that almost always needs closer review and/or investigation. These also almost always result in some form of enforcement action to properly respond to the significance of the noncompliance condition.
21-27	Serious (Yellow)	Closer review or investigation on the circumstances and extent of non-compliance should be undertaken. These can result in an enforcement action.
13-20	Marginal (Green)	Non-compliance condition that should be evaluated with contributing factors to the extent that information can be obtained from the DOE enforcement Coordinator and/or the Security Director on these factors. In some cases this could result in closer review and investigation, and may result in an enforcement action.
1-12	Low (White)	Non-compliance condition that should be evaluated with the contributing factors to the extent that information can be obtained from the DOE enforcement Coordinator and/or the Security Director on these factors. These may not result in a closer review or investigation, or subsequent enforcement action.

EA-13 Security Significance Screening (Cont'd)



Disclosures

Classification Issues (CI)

☐ Failure to Receive Classification Review	☐ Guidance Issue (Incomplete, Unclear, Unavailable)
☑ Information Compilation/Association	☐ Misclassification by Authorized Classifier
☐ Review by Unauth. Classifier (Classifier Didn't Have Proper Authority)	

Controlled Articles (CA)

☐ Camera	☐ Cell Phone	☐ Disc (CD/DVD/Floppy)		☐ Fitness Tracker
☑ Hard Drive/External HD		☐ Headphones / Ear Buds		☐ Hearing Aids/Med. Device
☐ Laptop	☐ SD Card	☐ Smart Watch	☐ Tablet/iPad	☐ Thumb Drive/Iron Key
☐ Other CA	[Describe "Other CA" here]			

Cyber (CYB)

☑ Unauthorized Use of a Classified System	☐ Unclassified Computer Used to Process/Store
☑ Inside the Firewall	☐ Outside the Firewall

Improper/Unauthorized Transmission (IUT)

☐ Chat App	☐ Database/Software System	☐ Email	☐ Fax
☐ Hand Carry	☐ Mail/Shipped/Express Delivery	☑ Network Location/Shared Drive	
☐ VTC	☐ Unsecure Phone/Conf. Call	☐ Virtual Meeting Platform (Teams, WebEx, Zoom, etc.)	

Other

☐ Classified Hardware (Computer/Hard Drive)	☑ Hard copy	☐ Improper Access Control	
☐ Improp. Escort	☐ Media Leak	☐ Open Source/Internet	☐ Parts / Matter
☐ Processing (Classified)	☑ Repository (VTR/Safe/etc.)		
☐ Other (Describe)	[Describe other disclosure here]		

Improperly Handled, Safeguarded, Secured, and/or Stored (HS)

☐ Destruction	☑ In Use	☑ Storage	☐ Reproduction	☐ Verbal/ Discussion
☐ Inventory of Accountable Matter		☐ Visual	☑ Unapproved Facility/Location/ Area (to Process/Store/Discuss)	

Causes

☐ Equipment/Material Problem	☐ Management Problem	☑ Personnel Error
☐ Procedural Problem	☑ Training Deficiency	☐ Design Problem
☐ External Phenomena	☐ Other	[Enter "other" description/details here]

Corrective Actions

☐ Communication Security System Mod.		☐ Cyber Security System Modification
☑ Training Mod.	☐ Disciplinary Action	☐ Physical Security System Modification
☑ Policy/Procedural Change	☑ Coaching/Counseling/Lessons Learned/Retrained	
☐ Other	[Enter "other" description/details here]	

Analyst Name	**Date**	**Analyst Comments**
Enforcement Officer Name	**Date**	**Enforcement Officer Comments**
Director Approval (for High Significance only)	**Date**	**Director Comments**

EA-13 Recommendation: ☐ Not 824/1017-Related (Delete) ☑ No Action (Add to SDB/ IOSC Wrap-Up) ☐ Enforcement Action (Add to SDB; Copy SSDW to Activity Folder)

Commonalities of a Good Screening Process

- Enforcement Staff intimately familiar with the regulations
  - Deployed staff may require nuclear safety, and worker safety and health training, and/or information security training
- Screen shortly after receipt to achieve timeliness
- Consistent use of a screening form
- Citations formatted to facilitate binning for trending
- Determine attributes for trending and make sure that the screening form addresses these areas
- Entry of the screen into the site issues management tool
- Easy access to Subject Matter Experts

Issues Not Reported in NTS and SSIMS

- All issues should still be screened and tracked
  - contractor's internal issues management system
- Tracking systems should include key information
- Compliance restored regardless of reportability

Expectations for Tracking

- All noncompliances tracked internally through issues management process
- Trending of noncompliances – may be performed in conjunction with Contractor Assurance Program
- Ensure that tracking systems help identify programmatic and repetitive issues

Trending Issues

EA-13

Total number of incidents

- Handling/Storage
- Cyber
- Classification Issues
- Controlled Articles with a Nexus to Classified

ORNL Sources of Noncompliances

- Occurrence Reporting & Processing System (ORPS)
- Local Issues Management System
  - Assessment & Commitment Tracking System (ACTS)
  - Assessment Results (Internal/External)
  - Training Deficiencies
  - Nonconformance Reports
  - Radiological Event Reports
- Laboratory Shift Superintendent Log
- Employee Concerns
- Enforcement Actions

ORNL - Screening of Potential Noncompliances

- Safety Regulatory Officers (SROs)
  - Approved SAP Role
  - Trained prior to role assignment
  - Deployed Lab-wide (~55)
  - ACTS Issues
  - Non-ACTS Screens
- Safeguards and Security
  - Screening of issues for Classified Information

ORNL - Trending

- ACTS screening results are compiled quarterly
- SROs provide quarterly summary of non-ACTS screens
- Screens are reviewed and compiled into a quarterly report
- Data is trended and reported via Contractor Assurance Processes
  - Monthly Operations Summary
  - Contractor Assurance Trimester Report
- Biannual Meeting
- Enforcement Actions

U.S. DEPARTMENT OF ENERGY

EA Enterprise Assessments

Questions?

Phase 3- Noncompliance Tracking Systems and SSIMS Reporting Closeout

Robert Smith
Enforcement Officer
Office of Worker Safety and Health Enforcement

Margaret Kotzalas
Enforcement Officer
Office of Nuclear Safety Enforcement

Charles Isreal
Enforcement Officer
Office of Security Enforcement

Tamara Baldwin
Enforcement Coordinator
Savannah River Nuclear Solutions

NTS and SSIMS
Reporting and Closeout Topics

- What does “voluntary” NTS reporting mean? Why report?
- Criteria/process for voluntary reporting of Part 824 noncompliances into SSIMS
- Process for drafting, reviewing, and submitting timely NTS and SSIMS reports
- Common elements and characteristics of a high quality NTS report and SSIMS report

NTS and SSIMS
Reporting and Closeout Topics (cont'd)

- Differences between "causal factors" and "noncompliances"
- How Extent of Condition reviews should be handled for NTS reporting purposes
- General criteria that the Office of Enforcement uses to evaluate Nuclear Safety and Worker Safety and Health NTS reports and SSIMS reports

U.S. DEPARTMENT OF ENERGY

EA Enterprise Assessments

Questions?

2024 DOE and Contractor Enforcement Coordinator Workshop

2:45 – 3:15	Break	
3:15 – 4:45	Case Studies | Worker Safety and Health	Room 6510
	Case Studies | Nuclear Safety	Room 6375
	Case Studies | Information Security	Auditorium
4:45 – 5:00	Feedback and Closing	Anthony Pierpoint, *Director* *Office of Enforcement*

2024 DOE and Contractor Enforcement Coordinator Workshop

Feedback and Closing

Anthony Pierpoint
Director
Office of Enforcement

U.S. DEPARTMENT OF ENERGY

EA Enterprise Assessments

We Value Your Feedback

Surveys

2024 DOE Safety and Security Enforcement Workshop website
https://ntc.doe.gov/EnforcementWorkshop