

Security Incident Management Program (SIMP)

at Sandia National Laboratories



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Typical Day in SIMP

- **Desk Inquiry Official (IO) receives all incoming pages.**
- **Desk IO processes all controlled article, stolen badge, and VTR variances.**
- **All other issues, such as Near Misses, Externals, and Incidents of Security Concern are transferred to the on-call IO.**
- **Categorization team meets to determine IMI categorizations.**
- **Attend RCA meetings.**
- **Meet with Managers for infraction determinations.**
- **Work with Classified Help Desk on email clean-ups.**
- **Write reports in the classified Safeguards & Security Information Management System (SSIMS).**

3 Variances

- **Controlled Article Variance - SO-SNL-08-012**
 - Self reported in a reasonable time frame
 - There was no potential for compromise of classified information
- **Stolen Badge Variance - SO-SNL-08-010**
 - The badge must not have been the target of the theft
 - The individual took reasonable means to protect the credential
- **Vault Type Room (VTR) Variance - SO-SNL-09-010**
 - One level of protection existed, either physical or electronic
 - The person does not have priors in last 24 months

Near Misses

- A barrier existed that prevented an incident from occurring, but is a indicator that an incident could occur in the future.
- Helps identify potential security issues that can be resolved before an incident happens.
- It is determined sometimes by luck that no compromise occurred because of barriers that existed.
- It is also determined based off of the aggravating and mitigating factors.

Incidents of Security Concern

- SIMP is required to categorize incidents based on DOE M 470.4-1, Section N, Impact Measurement Index (IMI) categories.
 - **IMI 1** – Actions, inactions, or events that pose the most serious threats to national security interests and/or critical DOE assets, create serious security situations, or could result in deaths in the workforce or general public.
 - **IMI 2** – Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations.
 - **IMI 3** – Actions, inactions, or events that pose threats to DOE security interests or that potentially degrade the overall effectiveness of the Department's S&S protection program.
 - **IMI 4** – Actions, inactions, or events that could pose threats to DOE by adversely impacting the ability of organizations to protect DOE safeguards and security interests.

Reporting Requirements

- SIMP has 24 hours to categorize an incident.
- SIMP then has to report the IMI to DOE Headquarters:
 - IMI 1 – 1 hour
 - IMI 2 – 8 hours
 - IMI 3 – 8 hours
 - IMI 4 – Monthly
- All Variances are reported monthly.

10 CFR 824

- Any incident that deals with classified information, regardless of compromise.
- FSO has target of 70 for fiscal year.
- Last year had 87 10 CFR 824 incidents, out of 202 total incidents.
 - Target was 80
- Had approximately 600 variances, majority were controlled articles.
- SIMP meets with Regulatory Support and updates them on major 10 CFR 824 incidents.
- FY2011, as of July 13, 2011, total 79:
 - IMI 1 – 1
 - IMI 2 – 3
 - IMI 3 – 21
 - IMI 4 – 54

FSO's role for Discipline

- Discipline for contract employees, not SNL.
- Help create corrective actions to prevent the event from re-occurring.

Call SIMP with Questions?

We would rather have you call our organization with a question that prevents an incident or mitigates it. Individual Inquiry Officials are here to help you!

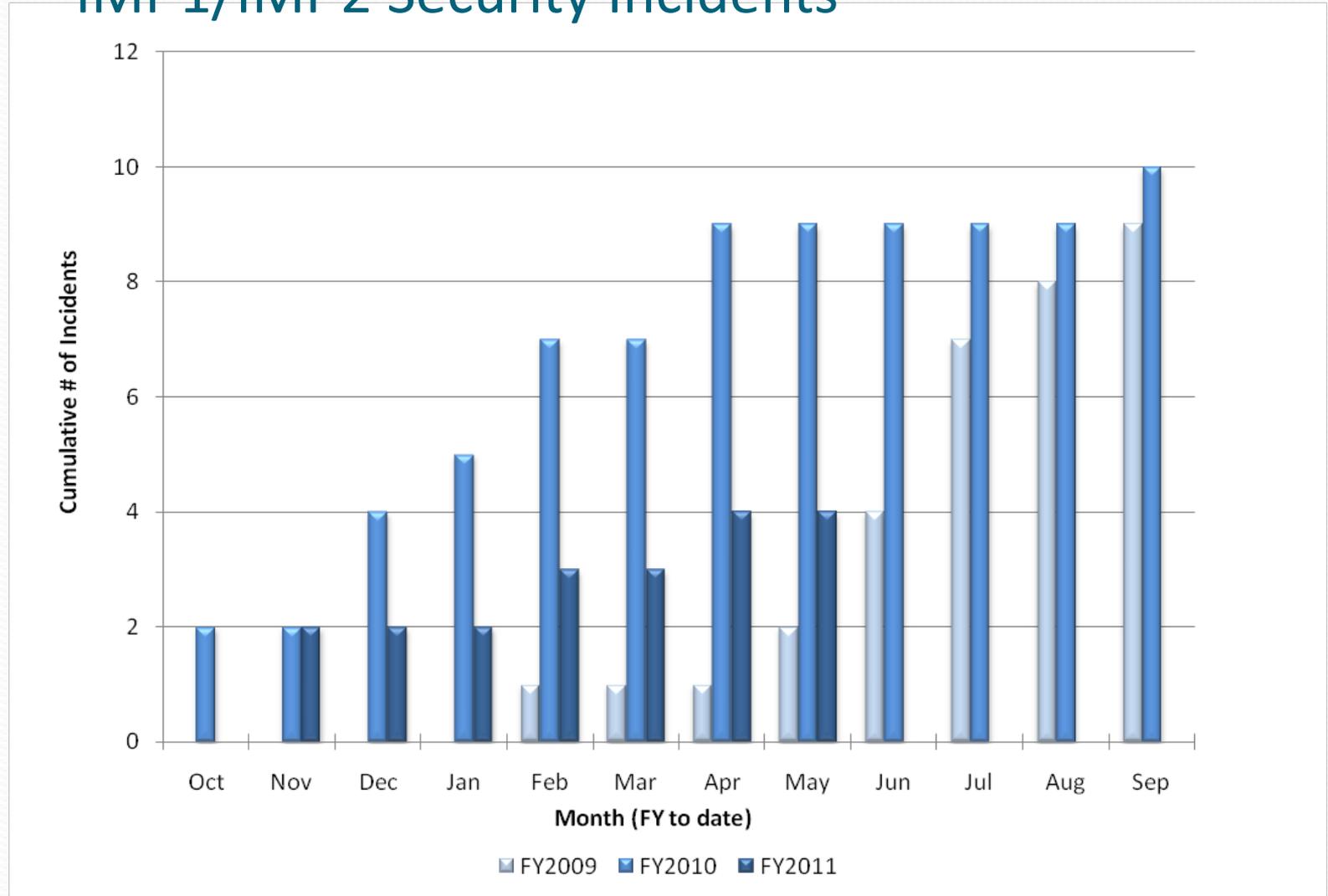
Incident Reporting (SIMP)

- NM: 505-540-2382
- CA: 888-932-9710

Non-Emergency (OOPS)

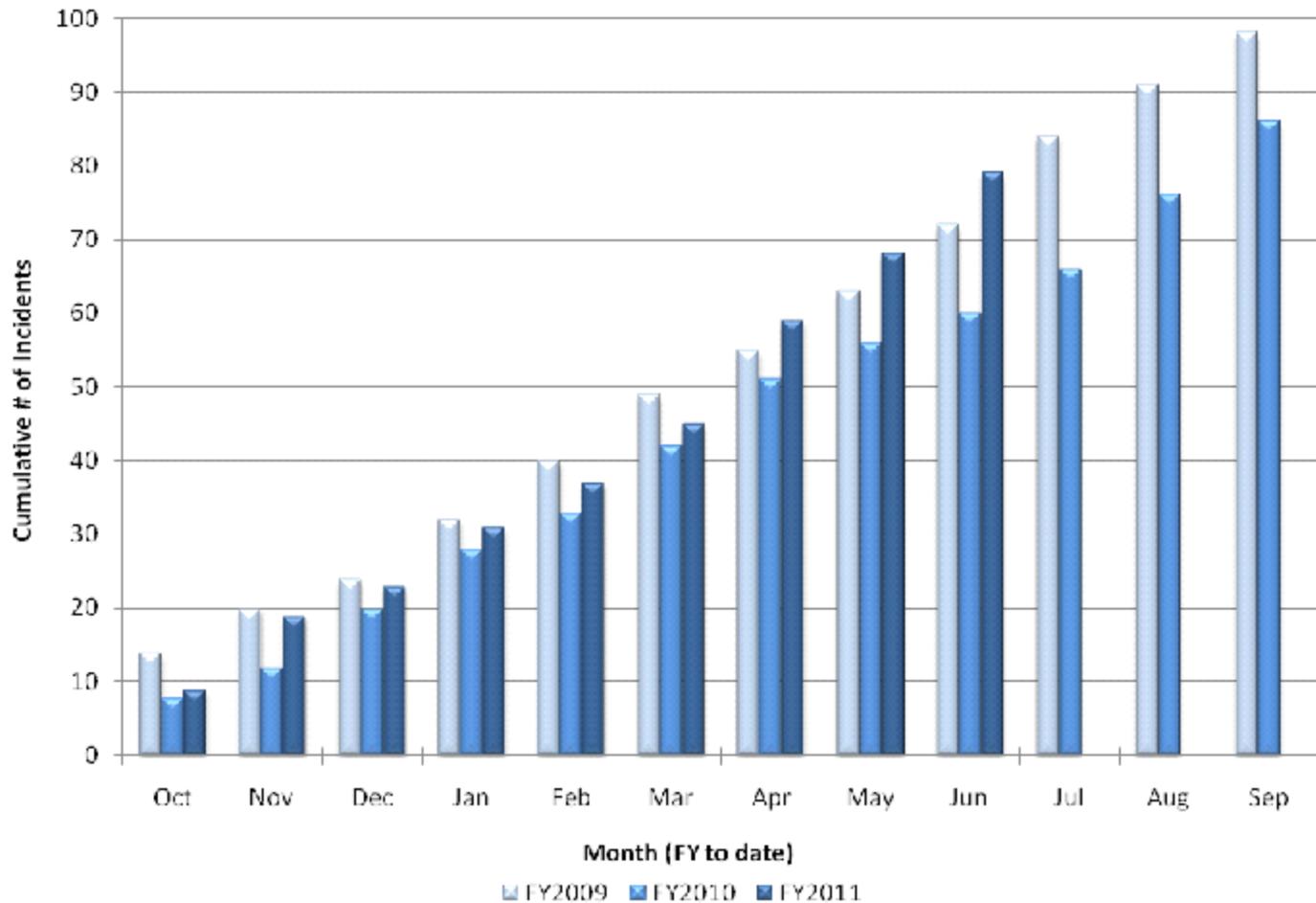
- NM or CA: 505-844-0311

Cumulative Trends for IMI-1/IMI-2 Security Incidents



FY11: 1 IMI-1 and 3 IMI-2 incidents

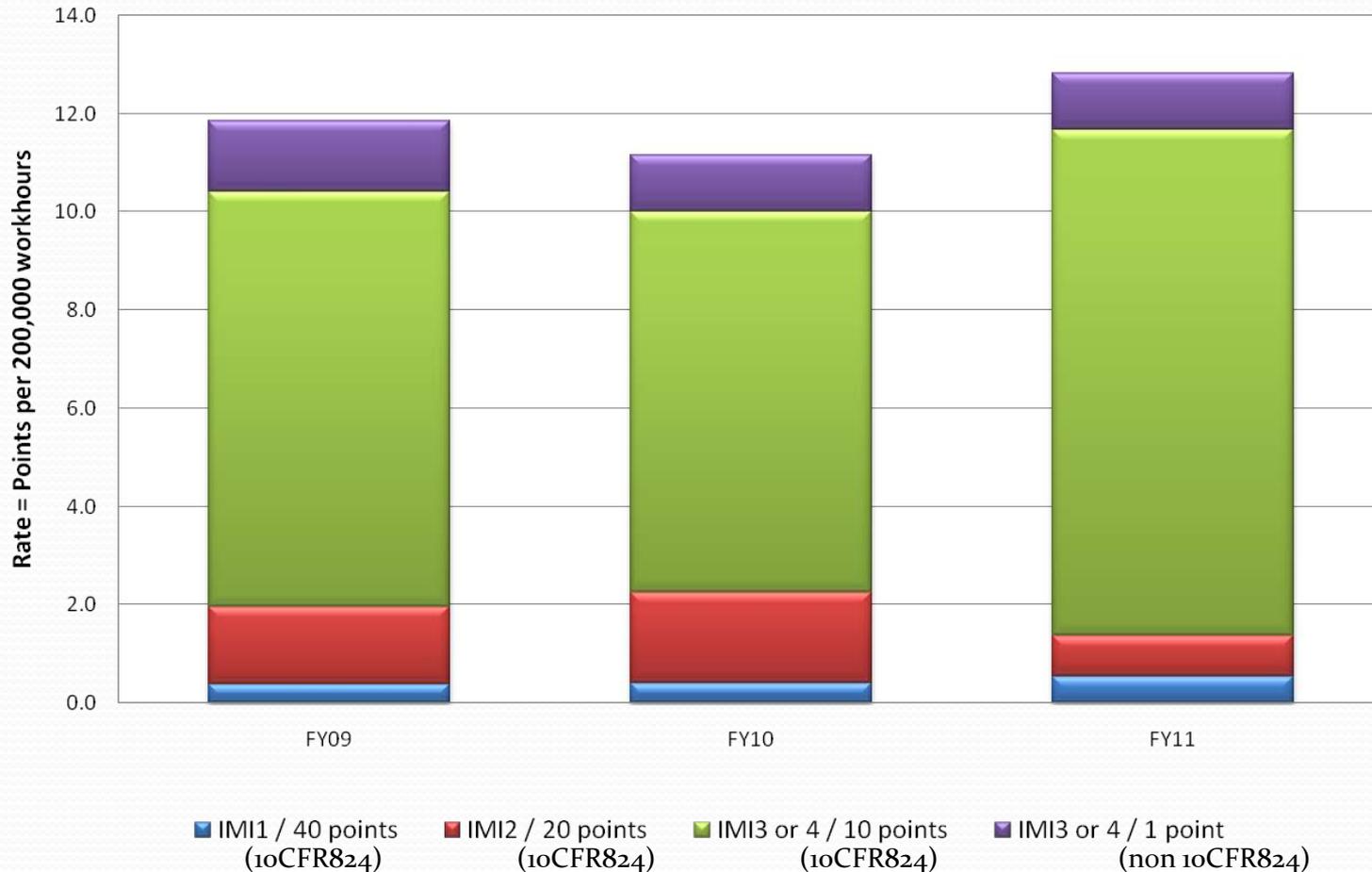
Cumulative Trends for 10CFR824 Security Incidents



-10CFR824 incidents are those of high risk which could relate to the protection of classified information and fall under the SIMP IMI categories of 1, 2 or 3.3, 3.4.0, 3.10, 3.18, 3.19, 4, 4.7, 4.13 (regardless of incident type) and could possibly result in fines.

-FY09 incidents, which would have qualified for current variances, are not shown in the above chart

Security Incident Rate



10CFR824 incidents are SIMP IMI categories of 1, 2 or 3.3, 3.4, 3.10, 3.18, 3.19, 4.0, 4.7, 4.13 (regardless of incident type).
-Hours are retrieved monthly from the ES&H Data Warehouse (see slide 7 for breakdown of hours)
-FY09 incidents, which would have qualified for current variances, are not shown in the above chart
The increase for FY11 is directly related to Email, VTR and Improper Storage incidents (10CFR824 incidents).

Causes

- Change in routine
- Not reporting incidents timely
- Inaccurate risk perception
- Time pressures
- Distracted

Behaviors

3 behaviors the SIMP team defined are:

- Managers should help their employees renew their perception of risk
- Individuals should also identify when their behaviors deviate from their routine
- Managers should also create an open environment by understanding that when employees are pressured for time.

Have a Security Attitude!

Think, Assess, Protect

- By integrating security into everyday tasks, you will help prevent potential incidents.
- STOP before conducting a task and think how does or how can this affect security?
- Remember: A double check should occur if you are rushed, in a hurry, out of your routine, or distracted. Most incidents happen because of one of these human factors.
- Identify latent conditions in your organization and work with your manager to correct them.
- SNL has a good reporting culture and it is moving toward great.

What Can FSOs do?

When FSO discuss security they should:

- Align their discussion with the mission values and expectations of the organization.
 - In order for Sandia to become a learning culture:
 - FSOs must ensure that when inadvertent mistakes are made they use it as a learning opportunity for their team.
 - Justice and Accountability should be reserved for reckless behaviors or individuals that have at-risk habitual behaviors.
- Recognize human errors. SNL has deviations in how to report incidents to DOE and can partner with you to ensure that your reporting is consistent with SNL.