Government Security Investigations

Lockheed Martin

Rotary and Mission Systems

Steve Fulton, RMS Orlando Facility Security Officer
Jon Bartley, RMS Threat Manager

Security Incidents

- **Security Infraction**
  - An incident involving a failure to comply with policy, process or procedure or the National Industrial Security Program Operating Manual that directly involves a misuse or mishandling of classified information, material or storage. The loss, compromise or suspected compromise of classified information is excluded by an investigation.
- **Security Violation**
  - An incident where the loss, compromise, or suspected compromise of classified information cannot be ruled out. A preliminary and final report to the Defense Counterintelligence and Security Agency is required.
- **Security Deviation**
  - A minor or administrative incident involving a failure to comply with LM policy, process or procedure that does not directly involve the misuse or mishandling of classified information, material or storage or the loss, compromise or suspected compromise of classified information.

Security Incident Job Aid, DCSA, CDSE, 15 April 2022

Prepare the Team

- In terms of pre-planning an ounce of preparation is worth a pound of cure
- Know your site and your resources
  - Understand who needs to know what and when
- Other than FSO and ISSM, consider SMO, IT Manager, Subject Matter Experts
- Do you have dedicated investigators? If you do, define swim lanes for the team
- Train users on what to do if they suspect a security incident – report to the FSO immediately

Plan Ahead

- Consider your facility and where the risk is for incidents
  - Do you have classified IS?
  - Are you a possessing facility or is access done elsewhere?
- Even without an IS, you should still have a plan to address incidents when they pop up
- Training employees to immediately report suspected incidents to FSO

Scenarios

- #1
  - –Classified document found unsecured on desk and a safe left open inside a classified space
    - The space does NOT have open storage approval
- #2
  - –Employee reports document she found on unclassified network has some concerning words- might be classified

Deviation, Infraction, or Violation?

- Do we have enough detail of incident to identify category?

- #1: Classified document found unsecured on desk of classified space without open storage approval, with safe found unsecured within the room.

- #2: Employee reports document she found on unclassified network has some concerning words- might be classified

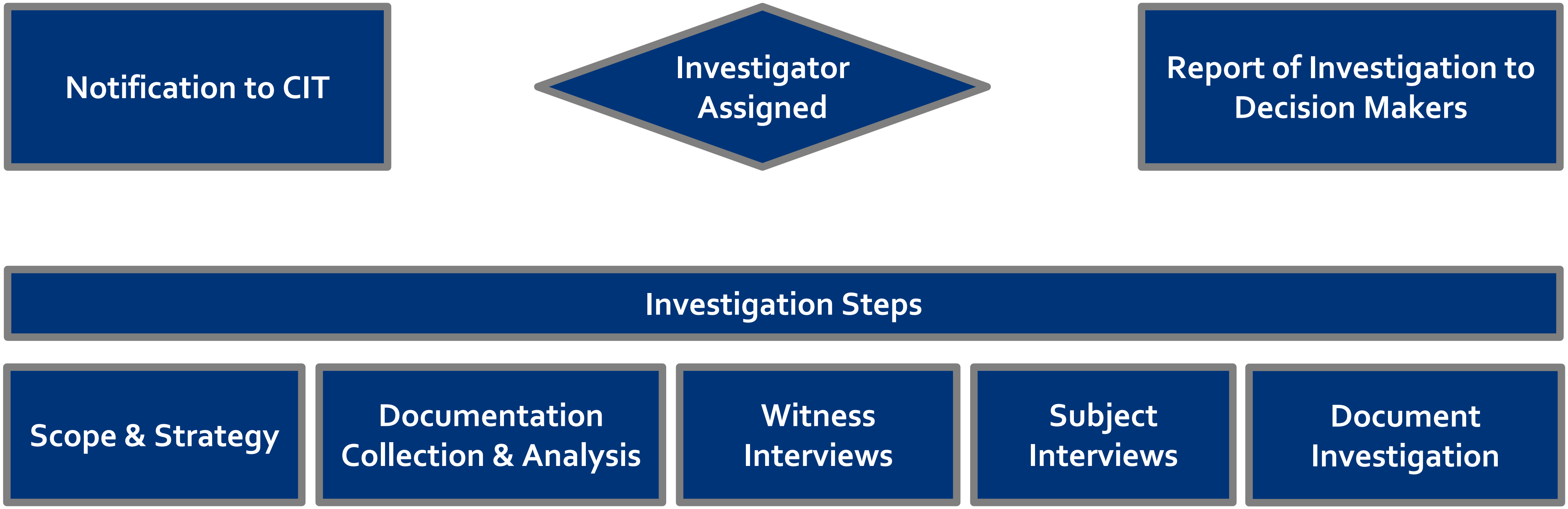
Initial Reporting/Steps

- Initial Steps
  - Inquiry phase with information gathering
    - This would likely include gathering statements from witnesses and other stakeholders
  - Will you need a subject matter expert/going to have to make classification decisions using SCG?
- Reporting on each incident
  - Anything due at this point
  - USG vs. Internal Stakeholders
- How they differ
  - Cyber incident adds complexity and risk
  - Incident one seems fairly straight forward, while the cyber incident is going to require additional work

Inquiry vs Investigation? Roles?

- Inquiry is done by FSO/ISSM/Program Security Staff and is initial fact finding and resource gathering
  - –702 forms, access logs, etc.
- RMS Centralized Investigations Team conducts investigation. Not the adverse piece, not the discipline piece- simply the facts!
- While conducting your investigations, keep that in mind- this is the fact finding, not the discipline

CIT Flow Chart



Notification to CIT

Investigator Assigned

Report of Investigation to Decision Makers

Investigation Steps

Scope & Strategy

Documentation Collection & Analysis

Witness Interviews

Subject Interviews

Document Investigation

Initial Inquiry Details

Incident 1

- Employee Ken Kennington signed the safe open the evening before you were notified
- The ACS shows Ken was the only person into the space the during the time frame the safe was open
- Ken did arm the IDS when he departed the space and it was armed with no alerts all night, per the alarm report

Incident 2

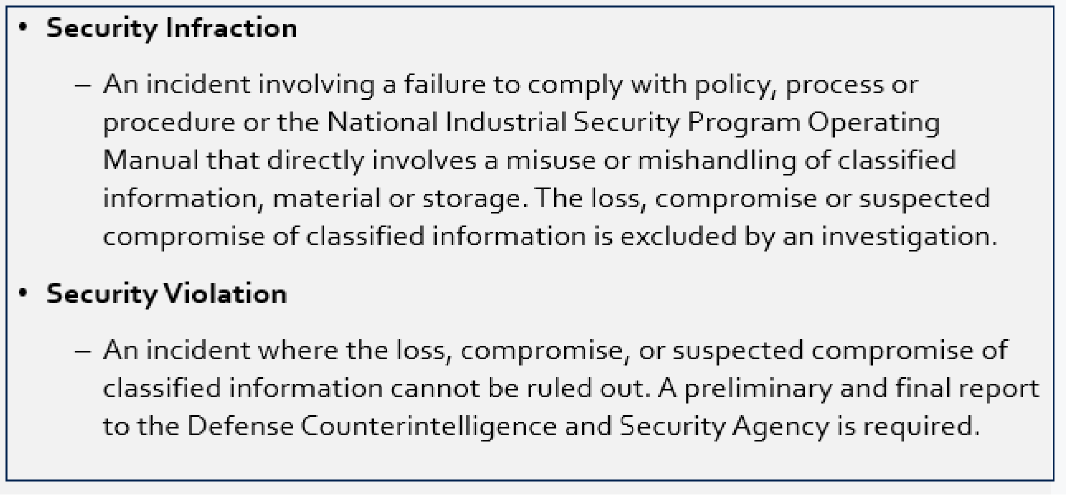
- FSO went to the unclassified terminal of employee Jan Jannington to perform a cursory look at the file that was already viewed
- FSO concurred the file was a concern but wasn't sure
- Need further clarification on classification
- DO NOT VIEW THE FILE ON ANY OTHER DEVICES

Deviation, Infraction, or Violation?

- Do we have enough detail of incident to identify category?

- #1: Classified document found unsecured on desk of classified space without open storage approval, with safe found unsecured within the room.

- #2: Employee reports document she found on unclassified network has some concerning words- might be classified



- **Security Infraction**
  - An incident involving a failure to comply with policy, process or procedure or the National Industrial Security Program Operating Manual that directly involves a misuse or mishandling of classified information, material or storage. The loss, compromise or suspected compromise of classified information is excluded by an investigation.
- **Security Violation**
  - An incident where the loss, compromise, or suspected compromise of classified information cannot be ruled out. A preliminary and final report to the Defense Counterintelligence and Security Agency is required.

Cyber Investigation

- If you have an ISSM- contact them
- You need to get a classification determination- that will guide next steps
- Two methods to determine information classification
  - Utilize Subject Matter Expert and Security Classification Guides to determine classification
  - Consult the data owner/customer using secure communication channels

Investigation Details

Incident 1

- FSO/Investigator interviewed Ken and he admitted he forgot to close the area properly
- He acknowledged the mistake he made and provided a written statement to that effect

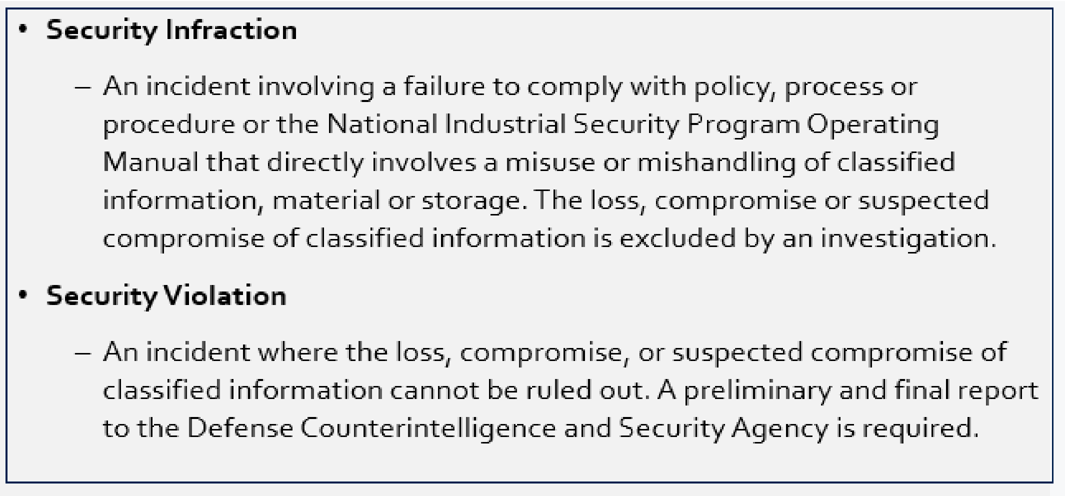
Incident 2

- Using the program SCG and subject matter expert that was properly trained to make derivative classification decisions confirmed the file in question was determined to be classified by compilation
- There is no document revision dates so unlikely to know who added the information that has contaminated the file

Deviation, Infraction, or Violation?

- Do we have enough detail of incident to identify category?

- #1: Classified document found unsecured on desk of classified space without open storage approval, with safe found unsecured within the room.
- #2: Employee reports document she found on unclassified network has some concerning words- might be classified



- **Security Infraction**
  - An incident involving a failure to comply with policy, process or procedure or the National Industrial Security Program Operating Manual that directly involves a misuse or mishandling of classified information, material or storage. The loss, compromise or suspected compromise of classified information is excluded by an investigation.
- **Security Violation**
  - An incident where the loss, compromise, or suspected compromise of classified information cannot be ruled out. A preliminary and final report to the Defense Counterintelligence and Security Agency is required.

Cyber Next Steps

- Initial report of violation to DCSA within applicable timelines
  - 1 calendar day after confirmation for TS
  - 3 calendar days after confirmation for S and C
- Engage the team- its time to clean up the network
  - IT needs to figure out who has viewed the file as assets will need to be collected
  - Is your network backed up anywhere? Tapes? Cloud backup? Where are those items physically located?
  - Refer to DCSA Incident Job Aid and your companies Spill Cleanup Procedures for how to best clean the network
  - Collect IT assets: laptops, hard drives, USB memory devices, smartphones that accessed the data. Protect them as classified material. Refer to DCSA ISR if you need storage options

Incident Details

Incident 1

- Investigation concluded
- Not a violation

Incident 2

- 3 company laptops were collected and secured as classified, awaiting destruction
- The IT team was able to perform a DCSA approved cleanup on the backups and the file was eradicated from the network
- No conclusive evidence was found to point to who added the material that made the document classified

Final Reporting

- Final report for violations required to be provided to DCSA within 30 days, but I have found there is some room for extensions- keep your ISR in the loop
  - This is where partnership with DCSA is crucial
- Refer to DCSA Job Aid for all details of final report
- Brief your site leadership
- Brief your customer/data owner/GCA
  - They are going to find out if they haven't already

Progressive Discipline and Tracking

- So far this has been all about the facts but industry is required to utilize a progressive discipline policy as well as track employees who violate security practices
- How does your company handle discipline for security incidents?
  - Committee?
  - FSO decides?
  - CEO decides?

LOCKHEED MARTIN

After Action

- Plan on DCSA reviewing all incident documents during SR or other engagements, to include memos detailing infractions
  - If you decided unilaterally it was an infraction- be prepared with evidence to back that up
- When planning, consider the new WFH stance by many employers and how you would handle remote work
  - What if an infected IT asset is located at an employee home 5 states away?
  - What if an employee emails a document to their personal email, accesses it on their phone and uses their personal printer to print it and it is noted as being part of a data spill?
  - Plan for contingencies

LOCKHEED MARTIN