SCENARIO 8 | DEFENSE AND AEROSPACE SUPPLIERS HANDLING CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Defense Supplier: CUI Exposure and DFARS Reporting

A defense supplier discovers that an engineering file share containing CUI was accessed by an unknown actor.

Suggested length	75 minutes	**NIST CSF 2.0 functions**	Govern, Respond

Exercise objectives

- Practice the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 72-hour reporting process
- Test evidence preservation and media retention requirements
- Review readiness for Cybersecurity Maturity Model Certification (CMMC) incident response requirements

Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

#	When	What happens
1	**Tuesday, 3:00 p.m.**	Your firewall vendor alerts on large outbound transfers from the engineering file server to an unfamiliar cloud storage service over the past week.
2	**Wednesday, 10:00 a.m.**	IT confirms the files include drawings marked CUI for a prime contractor's program. Nobody has a Department of Defense (DoD)-approved medium assurance certificate to log in to the DIBNet reporting portal.
3	**Thursday, 9:00 a.m.**	The prime contractor's security office calls asking whether you have had any incidents.

Discussion questions by role

Role	Questions
Security Lead / vCISO	• When does the 72-hour clock start, and who will submit the report?
IT Lead / MSP	• How do we preserve images of affected systems for at least 90 days?

Role	Questions
Executive Sponsor	• How do we communicate with the prime contractor?
Legal / Privacy Counsel	• What are our contractual obligations beyond DFARS?
Everyone	• What information do we need that we do not have? • Who outside the company must we contact, and do we have their numbers offline? • What would we do differently tomorrow?

Key decisions and good practices to look for

- Report to the DoD through DIBNet within 72 hours of discovery
- Obtain a medium assurance certificate before you need it
- Preserve images of affected systems and relevant monitoring data for at least 90 days
- Coordinate with the prime contractor as the contract requires
- Update the System Security Plan and Plan of Action and Milestones

Hotwash (last 15 minutes): What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.
Document it: the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.