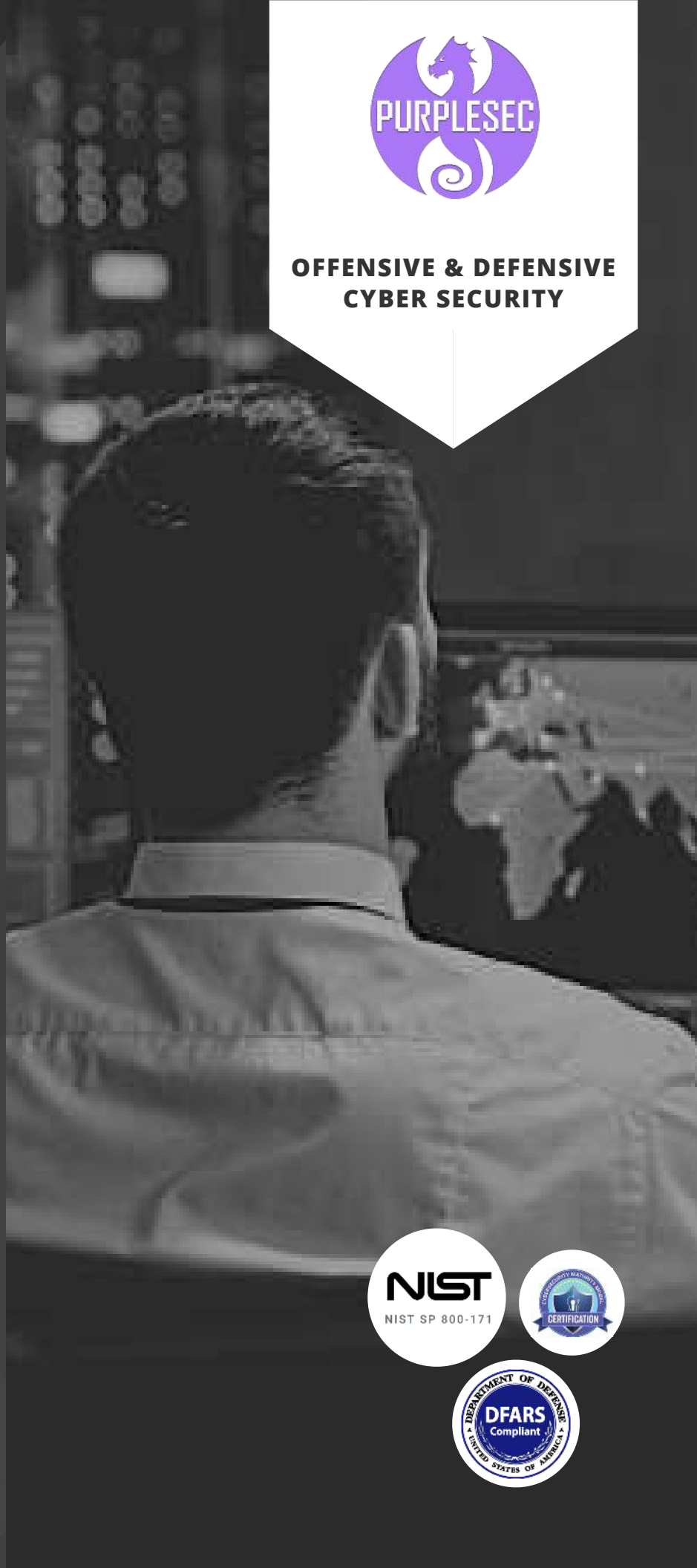
NIST

NIST 800-171 INCIDENT RESPONSE PLAN TEMPLATE

YOU'LL LEARN:

- What An Incident Response Plan Is
- NIST Incident Response Requirements
- NIST Incident Reporting Requirements
- What DoD Contractors Need To Report



PURPLESEC

OFFENSIVE & DEFENSIVE CYBER SECURITY

NIST SP 800-171

CERTIFICATION

DFARS Compliant

GET IN TOUCH

(202) 556-3903
sales@purplesec.us
purplesec.us

WHAT IS AN INCIDENT RESPONSE PLAN?

Are you prepared to successfully respond to incidents, whether they stem from malware, denial-of-service (DoS) attacks, stolen passwords, or lost laptops?

It's one thing to have security efforts in place to protect your data, but it's another to have incident response planning in place.

An incident response plan is a set of instructions designed to help IT staff identify, respond to, and recover from a security incident.

This plan refers to the scope of measures to be taken during an incident, not to the details of the incident itself.

A response plan for an incident is the instruction that the response team follows when an event occurs.

The purpose of an incident response plan is to protect sensitive data from a security breach, just as contingency plans are used to ensure the continuity of business processes and services during a malfunction.

NIST INCIDENT RESPONSE REQUIREMENTS

Incident response is one of the 14 requirements outlined in the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171—Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations, and enforced by the U.S. Department of Defense (DoD).

If your organization contracts for the government, you must implement all 14 of these requirements and security controls. Simply put, if you do not comply, you risk losing your contracts, costing your organization millions of dollars in lost revenue.

In the article Are You Ready for NIST 800-171 Compliance Marathon?, I walked through the NIST 800-171 security requirements. Now, I will tackle what compliance requirements are required for incident reporting.

WHAT IS A CYBER INCIDENT?

A cyber incident is defined as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

INCIDENT REPORTING COMPLIANCE REQUIREMENTS

According to NIST SP 800-171 section 3.6, the Incident Response family of security requirements focuses on establishing an operational incident-handling capability for organizational information systems that includes adequate:

- Preparation
- Detection
- Analysis
- Containment
- Recovery
- User response

You must acquire a medium assurance certificate to access the reporting site. So, this is the first step.

- Link to External Certification Authority Program
- DoD's Cyber Incident Reporting Page

Cyber incidents that impact a system within the scope of Defense Acquisition Regulations System (DFARS) must be reported within 72 hours of detection.

To report cyber incidents, you must have a medium assurance certificate. A review must be conducted so that the scope of the compromise can be understood.

At a minimum, this review must cover:

- Identification of affected systems
- Affected users accounts
- Affected data
- Other systems that might have been compromised

WHO SHOULD REPORT AND WHY?

- DoD contractors report cyber incidents in accordance with the DFARS Clause 252.204-7012
- DoD contractors report in accordance with other reporting requirements identified in a contract or other agreement
- DoD Cloud Service Providers report cyber incidents in accordance with clause 252.239-7010, Cloud Computing Services
- DoD's Defense Industrial Base Cybersecurity Program (DIB CS) Participants report cyber incidents in accordance with the Framework Agreement (FA)

The DoD has the right to request further information in order to investigate the cyber incident.

To this end, the contractor:

- Should take images of affected systems and any relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow the DoD to request the media or decline interest.
- Provide access to the DoD in order to carry out forensic analysis.
- Work with the DoD to provide any additional information that is required to complete the investigation.

WHAT DO DOD CONTRACTORS NEED TO REPORT?

DoD contractors shall report as much of the following information as can be obtained to DoD within 72 hours of discovery of any cyber incident:

Company Name	Company POC	Data Universal Numbering Sytem	Contract Numbers
Contracting Officer	USG Program Manager	Clearance (secret, top secret, etc.)	Facility CAGE Code
Facility Clearance Level	Impact to Defensive Information	Operational Support	Data Incident Discovered
Location(s) of Compromise	Incident Location CAGE Code	DoD Systems Involved	Type Of Compromise
Technique Use In Cyber Incident	Incident Outcome	Incident / Compromise Narrative	Additional Information

PURPLESEC

REPORT THE FIRE BEFORE IT SPREADS

While you may be doing what you can to prevent cyber fires from spreading and causing damage, there are procedures to follow to report the fire. If your clothes catch on fire, we all know about “Stop, Drop, and Roll.”

In the case of cyber incidents, it’s more like “Stop, Assess, and Report.”

Knowing and implementing the NIST 800-171 requirements—all 14 of them including incident response —is not only a good way to mitigate risk and minimize data exposure but critical to maintaining your organization’s compliance and status with the federal government.

REACH 100% COMPLIANCE MONTHS BEFORE THE AUDIT COMES

- **CONDUCT A CMMC GAP ANALYSIS**
- **IMPLMENT THE NIST 800-171 FRAMEWORK**
- **POAM&M AND SSP ASSISTANCE**
- **PASS AN UPCOMING CMMC AUDIT UP TO LEVEL 3**

GET A FREE CONSULTATION

PURPLESEC