

NIST 800 – 171 Incident Response Plan

Services	Deliverables
<ul style="list-style-type: none">NIST 800-171 Incident Response Plan	<ul style="list-style-type: none">Written Incident Response Plan

NIST 800-171 Incident Response Plan

This is the creation of a written Incident Response Plan that documents the processes and procedures for responding to security incidents involving systems that handle or store Controlled Unclassified Information (CUI), in accordance with the guidelines set forth in NIST SP 800-171 and NIST SP 800-61r (as directed by DFARS 252.204-7012). This document addresses the customer information network as a single system.

“Having a response plan in advance of an incident can make a world of difference.”



Objectives of this service:

- Define and document the roles and responsibilities of the company’s incident response handlers
- Describe the methodology and procedures for responding to incidents involving CUI to include:
 - Preparation
 - Detection
 - Containment
 - Investigation
 - Remediation
 - Recovery
- Document procedures for reporting and communicating incidents to outside parties
- Document plan to continuously improve incident response procedures

Upon completion the company will:

- Possess written Incident Response Plan
- Demonstrate to contract prime/DoD POCs company’s continued due care (‘reasonable person’ and ‘reasonable expectations’) through Business Impact Analysis and documentation of roles and responsibilities
- Be able to demonstrate to contract prime/DoD POCs company’s initial due diligence (ongoing effort) through incident response maturation plan

