Give Me 5 – Understanding Cyber Security
Protecting Unclassified Information
Incident Response Worksheet

National Institutes of Technology and Standards (NIST) Special Publication (SP) 800-171 defines the 14 families of security controls with which contractor information systems must comply. We will take a closer look at what is required to satisfy the requirements for Section 3.6, Incident Response.

What are the requirements?

3.6 INCIDENT RESPONSE

Basic Security Requirements:

3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

3.6.2 Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.

Derived Security Requirements:

3.6.3 Test the organizational incident response capability.

Figure 1 - Section 3.6, NIST SP 800-171

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.6 INCIDENT RESPONSE				
Basic Security Requirements				
3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. **3.6.2** Track, document, and report incidents to appropriate organizational officials and/or authorities.	IR-2	Incident Response Training	A.7.2.2*	Information security awareness, education, and training
	IR-4	Incident Handling	A.16.1.4	Assessment of and decision on information security events
			A.16.1.5	Response to information security incidents
			A.16.1.6	Learning from information security incidents
	IR-5	Incident Monitoring	*No direct mapping.*	
	IR-6	Incident Reporting	A.6.1.3	Contact with authorities
			A.16.1.2	Reporting information security events
	IR-7	Incident Response Assistance	*No direct mapping.*	

Figure 2 - Appendix D, NIST SP 800-171

© 2016 Ex Nihilo Management, LLC. All rights reserved

1. An organizational incident-handling capability requires _____ to report _____ _____ _____ to designated authorities.

2. An organizational incident-handling capability requires the _____ to report security incidents to _____.

3. In order to satisfy the requirement for Incident Response Training, you will, at a minimum need:
   - _____
   - _____
   - _____

4. Preparation may include developing _____, identifying _____ and _____, implementing _____ and processes to ensure timely reporting of security incidents.

5. Detection and analysis methods include:
   a. Antivirus protection, strong passwords, and firewalls
   b. Firewalls, routers and access control lists
   c. Passwords, firewalls and screen savers
   d. All of the above
   e. None of the above

6. Performing backups, changing passwords on compromised systems, gathering system logs, diagnosing or identifying the cause of the incident, are examples of _____.

7. To recover from a cyber incident, you will, at a minimum, need:
   - _____
   - _____
   - _____

8. Appropriate _____ techniques include the use of audit logs, intrusion detection systems, and other device monitors.

9. User response activities may include graceful degradation, _____ _____ _____, fall back to manual mode, employing _____ _____, alternate information flows.

10. Incident response testing includes, for example, the use of _____, walk-through or tabletop exercises, _____, and comprehensive exercises.

© 2016 Ex Nihilo Management, LLC. All rights reserved