FEDERAL AGENCY SECURITY REPORTING REQUIREMENTS

OMB Pushing for Improved IT Security Accountability

In the wake of recent data breaches, lost/stolen laptops and embarrassing "sting operations" of Government officials engaging in illegal cyber activities with minors, the White House's Office of Management and Budget (OMB) is now requiring agencies to be accountable for improved IT security. In July of 2006, OMB sent a memorandum to the chief information officers of all federal agencies notifying them that they must now report data breaches and violations of acceptable computing use policies to U.S. CERT (United States Computer Emergency Readiness Team).

OMB issued the memo despite the Federal Information Security Act of 2002 (FISMA) requirement that agencies report critical security incidents within an hour to the U.S. CERT. In fact, prior to the OMB memo, some agencies only reported cyber-security incidents to law enforcement and unfortunately others did not report the incidents outside of their agencies. NIST defines seven (7) federal agency incident categories for which agencies must report IT security incidents to U.S. CERT. Category 4 - Acceptable Use Policy (AUP) - violations much be reported weekly.

Despite FISMA and the recent OMB memo, many agencies have been slow to implement e-communications monitoring & control solutions that will give them insight into how their employees and contractors use the Internet and Government Off-the–Shelf (GOTS) desktops and laptops. The most common reasons for failure to implement appropriate safeguards have included:

- Legal concerns regarding employee expectation of privacy
- Concern with being seen as "Big Brother"
- Potential conflict with local unions
- Additional expense of implementing monitoring & control solutions

Regardless of the past reasons why many agencies have not enforced their AUP, it is now clear that the White House and U.S. Congress are stepping-up pressure to tighten internal security including levying penalties on agencies and individuals that fail to comply with published AUP's.

# # #

James Hackley is an EIM Advisor for Pearl Software, a Philadelphia-based software developer that produces Pearl Echo, an Employee Internet management tool. For additional information on how your agency can comply with the recent OMB acceptable computing use policies violation reporting guidelines, please contact James at James.Hackley@PearlSoftware.com.

Federal Agency Incident Categories

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	*Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

**Defined by NIST Special Publication 800-61*