

# Program Notice

GIPSA PN-04-05

01/23/04

---

## GIPSA COMPUTER INCIDENT RESPONSE PROCEDURES

### 1. PURPOSE

This program notice establishes the Grain Inspection, Packers and Stockyards Administration (GIPSA) cyber security computer incident response procedures and policy.

The purpose of an incident reporting policy is to facilitate cooperation and information exchange among all GIPSA personnel who have responsibility for detection, reporting, and notification of security incidents to management and legal authorities. This notice is issued to augment the following laws, regulations, directives: USDA Departmental Manual 3500, the Computer Security Act of 1987, National Institute of Standards and Technology Special Publication 800-3, and Office of Management and Budget Circular A-130, Appendix III.

### 2. EFFECTIVE DATE

This action is effective upon receipt.

### 3. BACKGROUND

Global network connectivity is common place for information exchange and is crucial for conducting everyday operations. However, the benefits can be overshadowed by the increase in network vulnerabilities. The number of Internet related incidents that have occurred in the past year, along with the increase and complexity of threats, requires that GIPSA take its incident handling capability seriously. Networks and IT resources are continually vulnerable to illegal/malicious activity or exploitation by internal and external sources. The most common security threats are to network systems. Network security threats include impersonation, eavesdropping, denial of service, and packet replay/modification. Damage to IT systems from a computer security incident (intrusion) can occur in a short period. Therefore it is essential that all GIPSA employees have procedures in place that can be activated immediately. The failure of an agency or mission area to promptly report an intrusion impacts and potentially compromises the Information Systems Security Program (ISSP) efforts of other USDA organizations and their customers.

#### 4. POLICY

All incidents that occur in GIPSA will be reported to the Information Systems Security Program Manager (ISSPM) or Information Systems Security Managers (ISSM's) immediately. When an incident is reported to an ISSM, he or she must inform the ISSPM as soon as possible. In the event the ISSPM/ISSM is not available, all incidents will be reported directly to the GIPSA Help Desk for appropriate action. In many cases, the ISSPM will then contact a member of Network Operations for action.

Intrusions, the focus of USDA Departmental Manual (DM)3500, are only one form of computer security incident. A computer security incident is any adverse event whereby some aspect of a computer system is threatened such as, loss of data confidentiality, disruption of data integrity, and disruption or denial of service. The types of incidents have been classified into low, medium, or high levels depending on the severity.

Low Level IT Incidents are the least severe and should be handled within one working day after the event occurs. These include:

- Loss of Personal Password
- Suspected Sharing of GIPSA Accounts
- Misuse of Computer Equipment
- Unsuccessful Scans/Probes
- Computer Virus/Worms (Level Depends on Impact to Agency/Department)

Medium Level IT Incidents are more serious and should be handled the same day the event occurs (normally in two to four hours of the event). These include:

- Unfriendly Employee Termination
- Violation of Special Access to a Computer or Computing Facility
- Illegal Building Access
- Unauthorized Use of a System for Processing or Storing USDA Data
- Property Destruction Related to a Computer Incident (Less than \$100,000)
- Personal Theft Related to A Computer Incident (less than \$100,000)
- Computer Virus/Worms (Level Depends on Impact to Agency/Department)

High Level IT Incidents are the most serious and considered “Major” in nature. Because of the gravity of the situation and the high potential for harm to USDA, these incidents should be handled as soon as possible. These include:

- Suspected Computer Break-In
- Denial of Service Attacks (Sending Invalid Requests so that Legitimate Users Cannot Access a System.)
- Computer Virus/Worms (Level Depends on Impact to Agency/Department)
- Unauthorized Use of a System for Processing or Storing Non-USDA or Prohibited Data
- Changes to System Hardware, Firmware or Software Without the System Owner's Authorization
- Property Destruction Related to a Computer Incident (exceeding \$100,000)
- Personal Theft related to a Computer Incident (exceeding \$100,000)
- Electronic Funds Transfer (EFT) File Exploitation/Manipulation
- Warez (Illegal Software Download/Sale)
- Child Pornography
- On-Line Gambling
- Pornography
- Download of copyright protected material
- Any violation of law

High Level "Major" IT Incidents which include Warez, Child Pornography, Pornography, Downloading Music/Unauthorized Software, any violation of law, or On-Line Gambling will be handled using an accelerated and confidential IT Incident Response. Suspected events of this nature are to be immediately reported to and coordinate with the Associate CIO for Cyber Security/Designate.

Other types of incidents include *isolated* viruses or misuse of computer equipment, unintentional actions, and common, unsuccessful scans or probes. The GIPSA ISSPM should consult with the Office of Cyber Security in determining whether these "other" incidents are High, Medium or Low. When faced with a security incident, GIPSA will respond in a manner that both protects its own information and helps protect the information of others that might be affected by the incident.

All incident response forms can be found in DM 3500.

## 5. QUESTIONS

Direct questions to the Information Systems Security Program at (202) 720-1741.

/s/ Donna Reifschneider

Donna Reifschneider  
Administrator