USDA COMPUTER INCIDENT RESPONSE PROCEDURES MANUAL

TABLE OF CONTENTS

Page

TABLE OF CONTENTS

CHAPTER 1 – GENERAL INFORMATION

Part I - Computer Incident Response Procedures

FIGURES

U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL MANUAL	Number: 3505-000
SUBJECT: USDA Computer Incident Response Procedures	DATE: 10/25/01
	OPI: OCIO, Cyber Security

CHAPTER 1

GENERAL INFORMATION

1 PURPOSE

This Departmental Manual establishes policy and procedures for reporting Major Information Technology (IT) incidents that may compromise the availability, integrity, and confidentiality of Department of Agriculture (USDA) IT and telecommunications resources. The purpose of an incident reporting policy is to facilitate cooperation and information exchange among all USDA personnel who have responsibility for detection, reporting and notification of security incidents to management and legal authorities. This manual is issued to augment the following laws, regulations, directives: 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 SPECIAL INSTRUCTIONS/CANCELLATION

This Departmental Manual replaces:

a OCIO Memorandum Final Agency Review Computer Incident Reporting Procedure dated 3/8/99;
b OCIO memorandum Incident Response Coverage, dated 6/29/99;
c OCIO memorandum Incident Response Coordination Center, dated 7/2/99.
d This chapter replaces Incident Reporting Procedures in DM 3140, ADP Security Manual and DR 3140-001 ADP Security Policy.
e This manual will be in effect until superseded.

3 SCOPE

This manual identifies the USDA's procedures for promptly reporting intrusions into Information Technology (IT) systems and establishes formal

reporting requirements for all such instances to the USDA Chief Information Officer (CIO). All security incident reports are to contain the facts and information needed to make informed management decisions and to assist in managing the resolution(s). This regulation applies to all USDA agencies, programs, teams, organizations, contractors, consultants, appointees, employees of USDA funded councils, associations, other government agencies and state/local governments and committees that use, process, manage USDA information or meet the requirements of "operator of a Federal computer System".

4 ABBREVIATIONS

CIO	- Chief Information Officer
CS	- Cyber Security
FBI	- Federal Bureau of Investigation
FTP	- File Transfer Protocol
I/D	- Intrusion Detection
IP	- Internet Protocol
IRT	- Incident Response Team
ISSO	- Information Systems Security Officer
ISSP	- Information Systems Security Program
ISSPM	- Information Systems Security Program Manager
IT	- Information Technology
NITC-SNCC	- National Information Technology Center – Systems Network Control Center
OCIO	- Office of the Chief Information Officer
OIG	- Office of the Inspector General
POC	- Point of Contact
OMB	- Office of Management & Budget
USDA	- United States Department of Agriculture

5 DEFINITIONS

Breach - Any illegal penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

Chain of Custody - Protection of evidence by each responsible party to ensure against loss, breakage, alteration or unauthorized handling. Protection also includes properly securing, identifying, and dating evidence. Individuals shall place their initials and date on the container when the evidence is stored in a container or on the evidence in such a way that no damage is incurred.

Compromise – A compromise is to invade something by getting around its security. A computer has been compromised, for example, when a Trojan Horse has been installed.
Compromise of Integrity – A compromise of integrity is any unauthorized modification of the correctness of information or data.

Computer Security Incident – A computer security incident is any adverse event whereby some aspect of a computer system is threatened: loss of data confidentiality, disruption of data or system integrity, disruption or denial of availability. Some examples are listed below:

Intrusion of computer systems via the network (often referred to as "hacking");
The occurrence of computer viruses and/or resulting damage;
Unusual or suspicious probes for vulnerabilities via the network to a range of computer systems (often referred to as scans);
Unusual processes, not installed by USDA, running on server.

Within the computer security arena, these events are often simply referred to as "incidents". The definition or identification of an incident may vary for each USDA agency or mission area depending on the situation. However, the following categories (also defined in this section) are generally applicable: Compromise of Integrity, Denial of service, Misuse, Damage, and Intrusions.

Damage – Damage is the unauthorized deliberate or accidental modification, destruction or removal of information or data from a computer system.

Denial of Service – Denial of service is an inability to utilize system resources due to unavailability; for example, when an attacker has disabled a system, a network worm has saturated network bandwidth, an IP address has been flooded with external messages or "a system manager and all other users become locked out of a UNIX system, which has been changed to single user mode."

Firewall - A security policy and technology that defines the services and accesses permitted, and an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall is to restrict access to or from a protected network. It implements a network access policy by forcing connections to pass through the firewall, where they are examined and evaluated. A USDA firewall must use stateful inspection technology that is

aware of the content and state of connection. This technology, which denies all traffic unless it is specifically allowed, employs rules targeted squarely at implementing security decisions at all levels; effectively log activities; filters throughout all levels of the protocol stack; tracks valid active sessions, and processes/filters/tracks high level applications such as electronic mail, file transfer and hyper-text transmission.

Harm – Harm is to damage, injure or impair Information Technology (IT) systems using electronic methods.

Incident Handling - This refers to the actions taken to resolve the incident.

Incident Oversight – This process is the ongoing surveillance of the networks and systems to spot new vulnerabilities and take corrective actions in advance of incidents.

Incident Reporting - This involves formal acknowledgement that a computer incident occurred.

Incident Response – This process is the analysis of how the incident happened and how to handle the situation so that it does not reoccur.

Intrusion – Intrusion is an unauthorized, inappropriate or illegal activity by insiders or outsiders that can be considered a penetration of a system.

Intruder - An intruder is a person who is the perpetrator of a computer security incident. Intruders are often referred to as "hackers" or "crackers." Hackers are highly technical experts who penetrated computer systems; the term Crackers refers to the experts with the ability to "crack" computer systems and security barriers. Most of the time "cracker" is used to refer to more notorious intruders and computer criminals. An intruder is a vandal who may be operating from within USDA or attacking from the outside of Department.

Level of Consequence - The impact an incident has on an organization. Impact includes: loss of data; the cost to a USDA agency or mission area; negative consequences to the organization (e.g. damage to reputation); and the magnitude of damage that must be corrected.

Misuse - Unauthorized use of an account by an intruder (or insider)constitutes misuse.

Need-to-Know - The necessity for access to, knowledge of, or possession of classified or other sensitive information in order to carry out officially

sanctioned duties. Responsibility for determining whether a person's duties require possession or access to this information rests upon the individual having current possession (or ownership) of the information involved, and not upon the prospective recipient. This principle is applicable whether the prospective recipient is an individual, a contractor, another Federal agency or a foreign government.

Threat – A threat is circumstance, condition, or event with the potential to cause harm to personnel and/or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste and abuse. The most common security threats are to network systems. Network security threats include impersonation, eavesdropping, denial of service, packet replay/modification.