FSIS DIRECTIVE	5420.6, Revision 1	1/26/2005

HOMELAND SECURITY THREAT CONDITION RESPONSE – INFORMATION TECHNOLOGY MONITORING PROCEDURES

I. PURPOSE

A. This directive details the emergency food security monitoring procedures that the Office of Management's Automated Information Systems Division (AISD) personnel will follow to protect the integrity of the information technology (IT) infrastructure in the event that a Threat Condition Elevated (Yellow), High (Orange) or Severe (Red) is declared by the Department of Homeland Security. In such an event, AISD personnel are to follow the instructions in this directive for the duration of the declared heightened Threat Condition.

B. This directive also:

• establishes how threat condition declarations will be communicated to AISD personnel; and

• provides specific instructions to AISD personnel on how to respond to threat condition declarations and changes in threat condition levels.

C. This directive does not address procedures to be followed in the event of an actual terrorist attack on FSIS facilities and related IT systems. Should such an attack occur, AISD managers will immediately take measures to protect the safety of AISD program personnel and notify the appropriate local authorities and the Director of AISD.

II. CANCELLATION

FSIS Directive 5420.6, dated 6/25/04

III. REASON FOR REISSUANCE

This directive is reissued in its entirety to provide clarification of responsibilities in the event of a Threat Condition Elevated (Yellow).

IV. REFERENCES

Directive 5420.1, Rev. 1, Homeland Security Threat Condition Response – Food Security Verification Procedures

---

DISTRIBUTION: Inspection Offices; T/A Inspectors; Plant Mgt.; T/A Plant Mgt.; TRA; ABB; TSC; Import Offices

OPI: OPPED

V. BACKGROUND

In 2002, the White House Office of Homeland Security established a Homeland Security Advisory System based on color to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. A declaration of a Threat Condition Yellow by the Department of Homeland Security indicates that there is an elevated risk of terrorist attacks. A declaration of a Threat Condition Orange by the Department of Homeland Security indicates that there is a high risk of terrorist attacks. A declaration of a Threat Condition Red reflects a severe risk of terrorist attacks. While the threat may or may not involve FSIS, the FSIS IT infrastructure, or food and agriculture sector specifically, it is imperative that AISD program personnel immediately undertake certain actions during such threat conditions to ensure the safety of critical FSIS IT systems and infrastructure. Because of the emergency nature of responding to a credible threat of a terrorist attack, AISD program personnel must clearly understand their roles and what will be required of them to properly respond to that threat should it arise.

VI. NOTIFICATION

A. In the event of a declaration of any Threat Condition:

- Elevated (Yellow), when there is a significant risk of terrorist attacks
- High (Orange), when there is a high risk of terrorist attacks, or
- Severe (Red) which reflects a severe risk of terrorist attacks,

by the Department of Homeland Security, the Office of Food Security and Emergency Preparedness (OFSEP) will inform the FSIS Administrator and senior executive leadership of all FSIS program areas. The Office of the Administrator will issue an e-mail letter to all employees notifying them of the heightened threat condition. Threat conditions will be announced by OFSEP and communicated to AISD personnel via e-mail, through the senior executive leadership in the Office of Management (OM). AISD program personnel should only begin implementing these procedures when instructed to do so by the AISD Program Manager (or his or her designee). In that event, AISD program personnel are to follow the instructions in this directive for the duration of the declared heightened threat condition. The nature of the work and location of AISD personnel during the performance of their assigned duties puts them in a position to identify threats to the IT infrastructure and to respond to stakeholders on IT security issues.

Upon notification by the AISD Director of the Heightened Threat Condition, AISD personnel will perform the security IT infrastructure monitoring procedures outlined in Section VII of this directive. Designated AISD personnel are to perform procedures daily for as long as the declared threat condition remains.

VII. IT INFRASTRUCTURE MONITORING PROCEDURES

A. The purpose of following emergency AISD IT security monitoring procedures is to provide assurance that there are no breaches in the security of Agency IT systems that could lead to actions compromising or damaging critical AISD systems. AISD personnel are to notify AISD management immediately of any observation of anomalies. The list of procedures outlined for each heightened threat condition is not all-inclusive. AISD personnel and managers will need to determine whether additional IT monitoring procedures are appropriate in their assigned areas of responsibility, and if so, what these additional measures are.

VIII. SPECIFIC THREAT CONDITION ACTIVITIES

Designated AISD personnel will take the following are the actions in the event of a declaration of:

A. Threat Condition Elevated (Yellow), High (Orange) or Severe (Red) with no specific threat to the food and agriculture sector.

Continue to observe IT operations for unusual activities.

B. Threat Condition High (Orange) with a specific threat to the food and agriculture sector.

1. Assess and determine if any preventative measures need to be applied to equipment or software.

2. Ensure availability of backup and recovery resources that may be needed.

3. Focus IT resources on network monitoring and immediately disconnect computer systems with suspicious network traffic. (Restoration of service will have the highest priority.)

4. Verify that network configurations are ready to implement for threat level Red.

5. Contact services and facilities that will be used if the threat level is increased to Red.

6. Ensure that System Administrators and technical support staff verify that all computer systems are at the appropriate version levels, including "patches."

7. Resolve any system aberrations detected in a security scan of each system.

8. Report all detected aberrations and means of resolution to the Director of AISD (or designee).

9. Monitor (by Staff Administrators and technical support staff) each computer

system's logs daily for any abnormal activity and report any suspect activity to the AISD security staff.

10. Conduct immediate security reviews using an auditing/assessment tool that will evaluate the network, provide reports to AISD management about security vulnerabilities on all critical systems, and apply any needed security patches.

11. Determine staffing availability for backup operations and notify the AISD personnel required to report for work.

12. Restrict access to computer rooms, communications closets, and critical operations areas.

13. Implement access restrictions and temporarily disable non-critical accounts.

14. Delay scheduled routine maintenance or non-security sensitive upgrades.

15. Provide guidance on use of alternative modes of communication and disseminate new contact information, as appropriate (i.e. cell phones, Blackberries, and teleconferencing).

16. Verify that Continuity of Operations (COOP) site is in stand-by mode and ready to take over.

17. Perform other necessary response procedures or modify the response procedures listed above as directed by the Department of Homeland Security or OFSEP.

C. Threat Condition Severe (Red) with a specific threat to the food and agriculture sector.

1. Provide 24/7 emergency tech support staff assistance.

2. Provide continuous 24/7 monitoring of intrusion detection and firewall logs.

3. Provide continuous 24/7 monitoring of security communications for latest vulnerability information.

4. Contact software vendors, where appropriate, for status of software patches and updates.

5. Move operations of mission-critical systems to back-up systems.

6. Disconnect non-essential network access where appropriate.

7. Initiate continuous monitoring of the network.

8. Verify that COOP site is in stand-by mode and ready to take over.

9. Verify that the USDA and FSIS COOPs are able to communicate with each other.

10. Perform other response procedures or modify the response procedures listed above as directed by the Department of Homeland Security or OFSEP.

D. AISD personnel are to immediately report any observations related to any potential breaches in IT infrastructure to AISD management and to OFSEP.

E. OFSEP will communicate the downgrading of a threat condition level to all AISD employees through the senior executive leadership in OM. Upon receiving such notification, AISD will return to prior operating procedures and advise all AISD personnel that normal operating procedures have resumed.

Direct all questions related to this directive through supervisory channels.

/s/ Philip S. Derfler

Assistant Administrator
Office of Policy, Program, and Employee Development