



United States
Department of
Agriculture

Grain Inspection,
Packers and Stockyards
Administration

Stop 3630
1400 Independence Ave., SW
Washington, DC 20250-3630

October 14, 2009

Reference # 223

TO: GIPSA POLICY BULLETIN BOARD

FROM: Frieda Achtentuch, Chief Information Officer /s/ *Frieda Achtentuch*
Information Technology Staff

SUBJECT: Personal Digital Assistant Travel Policy

ORIGINATING OFFICE: Office of the Administrator, Information Technology Staff

1. PURPOSE

The added portability and productivity enabled by Personal Digital Assistants (PDAs), such as the Blackberry, makes their use a business necessity. However, these devices extend beyond the boundary of the Grain Inspection, Packers and Stockyards Administration (GIPSA) infrastructure and inevitably add risk, which must be properly mitigated. One particular area of risk which must be addressed is the exposure of these devices to the multitude of threats prevalent while on international travel. In using these devices, due diligence is necessary to protect the GIPSA infrastructure and the integrity and confidentiality of information transmitted to and from them. The purpose of this document is to establish policy and provide direction and requirements for safeguarding GIPSA-issued PDAs taken outside the United States.

2. APPLICABILITY

The requirements set forth in this policy apply to all GIPSA employees who use GIPSA-issued PDAs (such as the Blackberry).

3. POLICY

All GIPSA employees traveling outside the United States (official or personal) with a GIPSA-issued PDA must have it scanned before and after the trip for security reasons. Employees must contact the Office of International Affairs to make arrangements for this to be done.

4. AUTHORITY

The GIPSA Chief Information Officer (CIO) has the authority to develop, implement, and manage IT security processes and procedures to protect the availability, confidentiality, and integrity of the Department's IT resources. The Office of the Chief Information Officer (OCIO) shall ensure that IT security policy and requirements are developed consistent with applicable statutory authority, including the Clinger-Cohen Act and the Federal Information Security Management Act (FISMA); with regulatory requirements and external guidance, including Office of Management and Budget (OMB) policy and Federal Information Processing Standards (FIPS) publications promulgated by the National Institute of Standards and Technology (NIST); and with internal policies and requirements.

5. REFERENCES

- a. OCIO Directive DM 3550-003, Portable Electronic Devices and Wireless Technology (February 8, 2006).
- b. NIST Special Publication 800-53 rev 1.
- c. Title I11 of the E-Government Act of 2002, the Federal Information Security Management Act (FISMA).
- d. OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)
- e. OMB M-06-16, Protection of Sensitive Agency Information (June 23, 2006)

6. QUESTIONS

Direct any questions concerning this policy to the GIPSA CIO at (202) 720-0265.