



Grain Inspection,  
Packers and Stockyards  
Administration

April 19, 2017

TO: GIPSA All

FROM: Daniel Knight  
IT Business Director  
Information Technology

SUBJECT: GIPSA Policy Statement on Pornography

Office of the  
Administrator

1400 Independence Ave.  
SW, Mail Stop 3647  
Washington, D.C. 20250

Voice 202-720-0219  
Fax 202-205-9237

Hotline 1-800-998-3447

[www.gipsa.usda.gov](http://www.gipsa.usda.gov)

Following the 2016 data breaches at the Office of Personnel Management (OPM), the U.S. Department of Homeland Security (DHS) began scanning all Federal agency IT networks, servers, and computer equipment that connect to Federal networks. The goal was to look for areas where we might be vulnerable.

Of surprise and great concern, DHS has detected numerous GIPSA employees accessing, viewing, downloading, and/or sending or receiving pornographic materials. In some cases, the accessed pornography has included potential or actual child pornography, a criminal offense pursued by the Department of Justice if confirmed to be child pornography.

This senseless and embarrassing use of our resources must stop immediately. In most GIPSA cases where such use is found, the employee is removed from Federal service. However, I have learned that some managers are not addressing this type of offense with the seriousness needed. In this regard, I am providing GIPSA employees with notice of a change in policy, in that cases involving pornography will be treated very seriously in the future, and that severe penalties, up to and including removal, are to be imposed regardless of penalties imposed prior to this notice.

Please do not forget that GIPSA owns the rights to all data and files in any computer, network, or other information system used and that each time you sign into the network, you are advised that the Agency can monitor electronic information and the use of the Internet and computer equipment. Even if an employee or contractor engages in conduct prohibited by this and other USDA policy during off-duty hours, such use is not excused. There is no expectation of privacy in any information or activity conducted, sent, performed, or viewed on or with government equipment or Internet access. Accordingly, employees and contractors should assume that whatever they do, type, enter, send, receive, and view on any GIPA electronic information system is electronically stored and subject to inspection, monitoring, and evaluation at any time.

Each of us has a responsibility to help ensure the security of our IT systems and to abide by the rules of conduct for Federal employees. In addition to pornography misuse, I wanted to take this opportunity to remind all GIPSA employees and contractors about other activities that are prohibited when using your government computer. The following activities and/or actions are misuses of government office equipment or government time – and in some cases, may be violations of law:

- Using government office equipment or government time for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, gender identity, national origin, sexual orientation, or engaging in any prohibited partisan political activity;
- Downloading copyrighted materials such as movies or TV shows using government equipment or government time; and,
- Using peer-to-peer or streaming services including, but not limited to, Pandora, Live 365, BitTorrent, or Spotify from your government equipment.

Several USDA Directives (DR), along with the Employee Rules of Behavior for IT Security, further describe your responsibilities when using information systems. You can find the links to the Directives below.

I take this opportunity to remind everyone that if there is anything negatively impacting you, it is the policy of GIPSA to offer counseling to all employees. The Employee Assistance Program (EAP) is a confidential service that can help in a variety of situations. The EAP can be reached at 1-800-222-0364.

Thank you for your help and support in protecting GIPSA by avoiding use of IT resources with unnecessary and destructive behaviors.

#### **USDA Directives**

- [Telecommunications & Internet Services and Use \(DR 3300-001\)](#) including the “[Limited Personal Use](#)” policy
- [Employee Responsibilities & Conduct \(DR 4070-735-001\)](#) specifically Item #16 “Use of Computers & Telecommunications Equipment”