U.S. Chemical Safety and Hazard Investigation Board

SUBJECT: Use of Government Office Equipment

CONTENTS

1. **PURPOSE.** This Order provides the policy of the Chemical Safety and Hazard Investigation Board (CSB) on the use of Government office equipment. This Order does not supersede any other applicable law or regulation. Authorities related to this policy are listed in Section 4.

2. **EFFECTIVE DATE.** This Order is effective upon passage by the Board and will remain in effect until superceded or rescinded.

3. **SCOPE.** This Order applies to all CSB employees and Board Members. Contractors are not authorized limited personal use of Government office equipment, unless a contract or other memorandum of agreement specifically permit it. Indiviudal Contracting Officer's Technical Representatives (COTR's) are responsible for addressing this issue in consultation with IT Security staff.

4. **REFERENCES.** This Order is based on relevant provisions of 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch, and on OPM's Policy on Personal Use of Government Office Equipment.

5. **DEFINITIONS.**

    a. **Government office equipment** – includes, but is not limited to: personal computers, related equipment and software, personal digital assistants, Internet services, email, library resources, telephones, pagers, facsimile machines, photocopiers and office supplies, which are provided by the government.

    b. **Minimal additional expense** – means the expense incurred when the Government is already providing equipment, supplies or services and you use only limited additional amounts of electricity, ink, toner or paper. Wear and tear from normal use is also considered minimal additional expense.

    c. **Non-work time** – means the time when you are not performing an activity for the benefit of the agency and under the control or direction of the agency. Examples of non-work time include off-duty hours such as lunch periods, before or after a workday, weekends or holidays, but only if your duty station would normally be available to you at such times.

    d. **Personal use** – means any uses other than official Government business.

    e. **Privilege** – means that you have no inherent right to personal use of Government office equipment.

6. **RESPONSIBILITIES.**

    a. **Human Resources Director** – the HRD will ensure that all current employees receive a copy of this Order. The HRD will ensure that all new employees receive a copy of this Order as part of the orientation process.

b. **Supervisors** – are responsible for fairly and equitably administering the provisions of this Order, and for reviewing and taking action when employees under their supervision are misusing Government office equipment.

c. **Employees** – are responsible for familiarizing themselves with, and following, the policies and procedures in this Order.

7. **POLICY. You may use Government office equipment only for authorized purposes.** *Limited personal use is authorized as follows*:

- Limited personal use is only authorized if it involves minimal additional expense to the Government.

- You are authorized to make limited personal use of Government office equipment during *non-work time*. For example, surfing the Internet during work time for non-work purposes is not appropriate.

- This use must not reduce your productivity or interfere with your official duties or the official duties of others.

- You must be authorized to use equipment for official Government business before it is available to you for limited personal use. Furthermore, CSB is not required to supply you with equipment if it is not required for you to perform official Government business.

- Supervisors may further restrict personal use based on the needs of the office or problems with inappropriate use in the office.

8. **NO EXPECTATION OF PRIVACY.** While using Government office equipment, your use *may be* monitored or recorded. All users of CSB office equipment should understand that they have no right or expectation of privacy while using any government office equipment at any time, including while accessing the Internet, using email, or any equipment for business purposes or for limited personal use. To the extent that CSB employees prefer that their non-government activities remain private, they should avoid using all CSB equipment, including the Internet, email, fax and telephone services. If Government office equipment or services are involved at any point in the transmission or receipt of information, then this policy applies and your use may be monitored. For example, if you use a Government PC to read or respond to personal email sent to you at a non-Government email address (e.g., AOL, Yahoo), your use may be monitored. By using the governement's computer system, system users are consenting to disclosing the contents of any files or information maintained in or on that equipment.

9. **MONITORING PRACTICES AND ACCESS CONTROLS.**

a. **Monitoring Practices** – There is no right or expectation of privacy in the use of government office equipment, and the CSB reserves the right to monitor all uses at any time. However, the CSB does not plan to routinely access or disclose the content of electronic communications of individual computer system users. Instead, the CSB IT security staff employ standard software to monitor network traffic patterns to maintain network security. IT security staff also employ software to block employee access to certain web sites that have no legitimate public purpose, such as those concerned with the distribution of pornographic material. Additional routine monitoring and/or access may be necessary, with or without notice, for other business purposes. Telephone and facsimile transmissions are not routinely monitored. The CSB reserves the right to monitor such transmissions to investigate misuse or misconduct, for other law enforcement purposes, or to otherwise defend the interests of the CSB.

b. **Access Authorization** – When required to investigate possible misuse, misconduct, defend the interests of the CSB, or for other lawful purposes, access to individual information technology systems, including access to individual user acitivity and information, is governed in accordance with Board Order 034, *Information Technology Security Program*. The procedures in that Order make it clear that only certain CSB officials are authorized to grant access to the CSB's electronic information systems. IT staff will continue to coordinate directly with individual users when access is required to an individual work station for routine maintenance such as installation of software upgrades.

10. **AVOIDING APPEARANCE THAT PERSONAL USE IS OFFICIAL.** An employee or Board Member must ensure that their personal use of government equipment does not give the appearance that they are acting in an official capacity. For example, an employee may not post CSB information to external news groups, web logs (blogs), bulletin boards or other public forums without CSB authorization. Further, an employee must not give the appearance that the CSB endorses or sanctions his or her personal activities. If an employee's actions leave the impression that his or her personal activities are endorsed by the CSB, the employee may be in violation of the standards of ethical conduct for executive branch employees. If there is any potential for confusion, an employee should provide an appropriate disclaimer. Here is an example of a disclaimer: "The content of this message is mine personally and does not reflect any position of the Government or of the CSB."

11. **EXAMPLES OF INAPPROPRIATE PERSONAL USE.** Employees must not use Government office equipment for activities that are inappropriate. If an employee has questions about appropriate use, the employee should consult with his or her supervisor, IT security staff, or the Designated Agency Ethics Official. If you receive an email message that harasses or threatens you, report it as soon as possible to your supervisor for technical or managerial follow up. Examples of inappropriate activities include:

- Using large files. Your activities might reduce the effectiveness of a CSB system if you use large files. For example, sending or receiving greeting cards, video, sound, interactive games or other large file attachments may hinder the performance of an entire network. You should not subscribe to Internet services that automatically download information, such as sports scores, stock prices or other continuous data streams, such as music or videos.

- Loading personal software onto your computer or making configuration changes. For example, computer games, personal tax programs and personal schedulers may not be loaded on CSB computers, and their use on CSB systems is prohibited.

- Engaging in email practices that involve ongoing message receipt and transmission, referred to as "instant messaging."

- Making personal long distance telephone calls. There are three exceptions:

  - in an emergency,
  - brief calls within the local commuting area to locations that can only be reached during working hours (e.g., car repair shop, doctor), and
  - brief calls home within the local commuting area (e.g., to arrange transportation, check on a sick child).

- Using Government equipment as a staging ground or platform to gain unauthorized access to other systems.

- Creating, copying or transmitting chain letters or other mass mailings, regardless of the subject matter.

- Creating, copying or transmitting any material or communication that is illegal or offensive to fellow employees or to the public, such as hate speech, material that ridicules others based on race, creed, religion, color, sex, disability, national origin or sexual orientation.

- Viewing, downloading, storing, transmitting or copying materials that are sexually explicit or sexually oriented, related to gambling, illegal weapons, or any other prohibited activities.

- Using Government office equipment for commercial purposes or in support of other "for profit" activities such as outside employment or businesses (e.g., selling real estate, preparing tax returns for a fee).

- Using government equipment to engage in any outside fund raising activity, endorsing any product or service, participating in lobbying or prohibited partisan

political activity (e.g., expressing opinions about candidates, distributing campaign literature).

- Acquiring, reproducing, transmitting, distributing or using any controlled information including computer software and data, protected by copyright, trademark, privacy laws, other proprietary data or material with other intellectual property rights beyond fair use, or export-controlled software or data.

12. **PENALTIES FOR MISUSE OF GOVERNMENT EQUIPMENT.** Unauthorized or inappropriate use of Government office equipment may result in the loss or limitation of your privileges. You may also face disciplinary action ranging from counseling to removal from the CSB, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

13. **INFORMATION SECURITY.** If you are using Government office equipment, particularly computer systems, you share the responsibility for protecting the security of this equipment with all other users. You must be aware of and follow appropriate security provisions concerning logging on or off CSB computer systems and networks. You are responsible for maintaining the confidentiality of your password and for all data that you place on or delete from a CSB computer. Because most CSB computers and systems are protected from unauthorized users by passwords, it is particularly critical that you not divulge your password to anyone. You should report all security breaches, including compromised passwords, to your supervisor, and to IT security staff. CSB Information Security responsibilities are more fully discussed in Board Order 034, *Information Technology Security Program*.

U.S. CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD

February 23, 2004