Registration and Evaluation System (RES)

Rules of Behavior

1.0 INTRODUCTION

Persons with access and accounts on the REGISTRATION and EVALUATION SYSTEM (RES) shall be held accountable for their actions related to the information resources entrusted to them. These personnel must comply with the following rules or risk losing their privileges and/or be subject to disciplinary action for failure to comply with these responsibilities. The Rules of Behavior apply to users at their primary workplace and at any alternative workplaces (e.g., telecommuting from home or from a satellite site). They also apply to users on official travel. These Rules of Behavior are consistent with IT security policy and procedures within DHS Management Directive 4300.1 (Information Technology Systems Security), DHS Sensitive Systems Policy Directive 4300A, and the DHS 4300A Sensitive Systems Handbook.

2.0 APPLICATION RULES

2.1 Telecommuting (Working at Home, at a Satellite Center/Office or Contractor Facility)

Employees approved for telecommuting must adhere to the following rules of behavior:

- I will physically protect any laptops or PEDs I use for telecommuting when they are not in use.
- I will protect sensitive data at my alternate workplace. This includes properly disposing of sensitive information (e.g., by shredding).
- I understand and will comply with the requirement that sensitive information stored on any laptop computer used in a residence or on travel shall be encrypted using FIPS 140-2 *Security Requirements for Cryptographic Modules* approved encryption.
- I understand and will comply with the requirement that sensitive information processed, stored, or transmitted on wireless devices must be encrypted using approved encryption methods.

2.2 Internet and E-mail Use

- I understand that my access and use of RES resources may be monitored, and I consent to this monitoring.
- I will not use peer-to-peer (P2P) file sharing to connect remotely to other systems for the purpose of sharing files. I understand that P2P can be a means of spreading viruses over DHS networks and may put sensitive government information at risk. I also understand that DHS Sensitive Systems Policy Directive 4300A prohibits the use of P2P software on any DHS controlled or operated equipment.

- I will not provide personal or official DHS information solicited by e-mail. I will be on alert if I receive e-mail from any source requesting personal or organizational information. If I receive an e-mail message from any source requesting personal information or asking to verify accounts or security settings, I will send the questionable e-mail to the appropriate security and/or system contact for verification as well as report the incident to the RES ISSO.

2.3 Software

- I agree to comply with all software copyrights and licenses.
- I will not install unauthorized software (this includes software available for downloading from the Internet, software available on DHS networks, and personally owned software) on DHS or DHS contractor equipment (e.g., servers, workstations, laptop computers, PEDs).

2.4 Passwords and Other Access Control Measures

- I will choose complex passwords that are at least eight characters long and have a combination of letters (upper- and lower-case), numbers, and special characters. I will not use a dictionary word, proper noun, name of person, pet, child or fictional character, my username, social security number, employee ID number, birth date, phone number or any other personally identifiable information as my password.

- I will protect passwords and access numbers from disclosure. I will not share passwords. I will not provide my password to anyone, including system administrators. I will not record passwords or access control numbers on paper or in electronic form and store them on or with DHS or DHS contractor workstations, laptop computers, or PEDs. To prevent others from obtaining my password via "shoulder surfing," I will shield my keyboard from view as I enter my password.

- I will change my password at least every 180 days or when prompted to do so by the Registration and Evaluation System and will not use the same or previous 8 passwords.

- I will promptly change a password whenever the compromise of that password is known or suspected.

- I will not attempt to bypass access control measures in place for the RES.

2.5 System Access

- I understand that I am given access to only those systems for which I require access to perform my official duties.
- I will not attempt to access data or systems I am not authorized to access.
- I will not provide or knowingly allow other individuals to use my account credentials to login to RES.
- I will not engage in, encourage, or conceal any hacking or cracking, denial of service, unauthorized tampering, or unauthorized attempted use of (or deliberate disruption of) any data or component within RES.
- I agree to inform my management or that of the Registration and Evaluation System when access to a particular computer resource is no longer required, such as when I have completed a project or no longer support an information resource.

- I agree that I have completed Computer Security Awareness training prior to my initial access to RES and that as long as I have continued access to RES, I will complete Computer Security Awareness training on an annual basis.

2.6 Accountability

- I understand that I have no expectation of privacy while using any RES equipment and while using services or programs provided by RES.
- I understand that I will be held accountable for my actions while accessing and using the RES and connected DHS systems and IT resources.

2.7 Incident Reporting

- I will promptly report IT security incidents, or any incidents of suspected fraud, waste or misuse of systems to the appropriate officials.

2.8 Data Protection

- I will use only DHS or DHS contractor office equipment (e.g., workstations, laptops, PEDs) to access DHS systems and information; I will not use personally owned equipment.
- I will protect sensitive information from disclosure to unauthorized persons or groups and will maintain control over, protect and mark sensitive Government material and resources appropriately. I agree to destroy physical documents and electronic media that may contain RES information, Sensitive but Unclassified (SBU) or For Official Use Only (FOUO) information by physical destruction (including pulping and shredding), degaussing or other media sanitization methods which meet DHS standards.
- To prevent and deter others from gaining unauthorized access to sensitive RES resources, I will log off or lock my workstation or laptop computer, or I will use a password-protected screensaver, whenever I step away from my work area, even for a short time; I will log off when I leave for the day.
- I agree not to use wireless connections to transmit RES information and data unless it is encrypted end-to-end using a FIPS-validated cryptographic method.
- I will not access, process, or store classified information on DHS office equipment that has not been authorized for such processing.

3.0 REGISTRATION and EVALUATION SYSTEM Rules of Behavior Statement of Acknowledgement

I have read and agree to comply with the requirements of the RES Rules of Behavior. I understand that the terms of this agreement are a condition of my initial and continued access to the Registration and Evaluation System and related services and that if I fail to abide by the terms of these Rules of Behavior, my access to any and all RES information systems may be terminated and that action, up to and including legal action, may be instituted against me. I have read and presently understand the above conditions and restrictions concerning my access to the Registration and Evaluation System.