Nuclear Regulatory Commission
Computer Security Office
Computer Security Checklist

Office Instruction:	**CSO-CKLT-1003**
Office Instruction Title:	**NRC General User Remote Access Computer Security Checklist**
Revision Number:	**1.1**
Effective Date:	**December 1, 2014**
Primary Contacts:	**Kathy Lyons-Burke, SITSO**
Responsible Organization:	**CSO/PST**
Summary of Changes:	CSO-CKLT-1003, "NRC General User Remote Access Computer Security Checklist" provides the computer security information that must be completed as a component of any approval for a general user to access NRC computing equipment and networks remotely.
Training:	Upon request
ADAMS Accession No.:	ML14301A055

Concurrences			
Primary Office Owner	Policy, Compliance, and Training		
Responsible SITSO	Kathy Lyons-Burke		**Date of Concurrence**
Directors	CSO	Tom Rich **/RA/**	29-Oct-14
	PCT	Kathy Lyons-Burke **/RA/**	29-Oct-14
	CSA	Thorne Graham **/RA/**	29-Oct-14

Concurrence Meeting Conducted via eMail			
Attendees:	Tom Rich	Kathy Lyons-Burke	Jon Feibus
	Thorne Graham		

Computer Security Checklist
CSO-CKLT-1003

NRC General User Remote Access Computer Security Checklist

---

1 PURPOSE

CSO-CKLT-1003, "NRC General User Remote Access Computer Security Checklist" provides the computer security information that must be completed as a component of any approval for a general user to access NRC computing equipment and networks remotely.

This front matter provides information to the user and should be removed prior to submitting the checklist as part of a remote access request.

2 GENERAL REQUIREMENTS

Any general user must successfully complete this checklist prior to obtaining approval to access NRC computing equipment and networks remotely. This checklist is one component of the approval process and does not constitute the only criteria used to approve a request. The following checklist assesses the security of the computing equipment at the alternate duty station.

3 SPECIFIC REQUIREMENTS

Users must be aware that vulnerabilities in the computer used to process NRC information places that information and the NRC infrastructure to which it connects at significant risk. Appropriate computer security protections are required to reduce the potential for malicious acts that can place NRC and the public at risk. All NRC equipment must be in compliance with NRC computer security policy and standards.

The requester's signature attesting to the accuracy of the information is required on the checklist after completion.

3.1 Operating System

This section addresses operating system settings and ensures that the operating system is configured appropriately and the user account is appropriate for access to NRC computers and networks. Vendor web pages provide information on whether or not the vendor is actively supporting an operating system.

A privileged account is defined in the NRC Agency-wide Rules of Behavior for Authorized Computer Use.

3.2 Anti-Virus

Anti-virus products (e.g., Norton Anti-virus, McAfee) intercept information received by the computer that contain codes referred to as signatures that are unique to a virus. Since new viruses are created every day, the product provided signatures must be updated frequently on the computer. The vendor web site indicates whether or not the vendor is actively supporting a

particular product. If the product is not actively supported, the product is not protecting against new viruses.

3.3 Anti-Spyware

Anti-spyware products (e.g., Spy Sweeper, XoftSpySE, Windows Defender) detect spyware using codes referred to as signatures that are unique to a type of spyware. Since new spyware are created every day, the product provided signatures must be updated frequently on the computer. The vendor web site indicates whether or not the vendor is actively supporting a particular product. If the product is not actively supported, the product is not protecting against new spyware.

3.4 Email

Email is used frequently to perform work. Malicious users know this and use email as a method of tricking users in a way that allows the malicious users to perform malicious acts. Links within emails can cause execution of malicious code unbeknownst to the user clicking on the link or may take the user to a web page that in turn executes malicious code or tricks the user into believing the web page is really a reputable bank or company.

3.5 The Web

Web sites are often used to trick users into clicking on links or ads that can cause the computer harm. For example, users are warned about their computer being infected with malware or that their computer performance can be enhanced and are offered free or low price software to help them resolve the issue. The software is really malware that infects the computer.

3.6 Personal Firewalls

Firewalls (e.g., Windows, Norton, McAfee) help the user screen out unwanted access to their computer. Firewalls can be configured to ensure another computer cannot access your computer as well as preventing certain types of known attacks.

3.7 Wired or Wireless Router

NRC provides router configuration requirements that help to protect the computer and users attached to the router. Routers are frequently attacked using default and weak passwords. Wireless routers are also attacked when they use weak wireless protocols. Types of router configurations that may exist include:

- a wired router, which consists of a cable from the router to a desktop;
- a router configured for wireless access that connects wirelessly to a laptop or tablet; or
- both a wired and a wireless connection (where the router has a cable to a desktop and wireless enabled to allow connections to other items (laptop, ipad, smartphone, etc)) This configuration is not permitted and either the wired connection or the wireless connection must be disabled.

All cybersecurity standards are identified on the CSO standards webpage located at: http://www.internal.nrc.gov/CSO/standards.html The relevant home router standards are identified on this page as: CSO-STD-1801, :Home Wireless Network Configuration Standard" and CSO-STD-1802, "Home Wired Network Configuration Standard." A link to the actual standards in the SharePoint repository is located just before the table on that page: CSO Standard Repository.

CSO-CKLT-1003 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
19-Apr-10	1.0	Initial Release	CSO web page	
29-Oct-14	1.1	Added separate items to reduce confusion	Posting to CSO web page and notification to ISSOs.	Upon request

NRC General User Remote Access Computer Security Checklist (Version 1.1)	
Operating System	
☐ Yes ☐ No	Any NRC computer being used is in compliance with the NRC cyber security policy and standards.
☐ Yes ☐ No	The computer account being used to perform NRC work is not a privileged account.
☐ Yes ☐ No	The computer being used has an operating system and applications that are still actively supported by the vendor (e.g., not old enough to be unsupported).
☐ Yes ☐ No	Computer security patches and updates to the operating system (e.g., Windows Operating System) and applications (e.g., Microsoft Office, Adobe Reader) are applied before performing NRC work.
☐ Yes ☐ No	I understand that Microsoft will never send out updates and patches, or announcements about updates and patches, via email and I agree not to click on a link within an email that purports to provide them.
☐ Yes ☐ No	I have configured Windows to show all file extensions so that I understand the type of file I am accessing.
☐ Yes ☐ No	Passwords for all administrative accounts to which I have access use strong passwords (per CSO-STD-0001).
☐ Yes ☐ No	I changed all default passwords on my computer to be strong passwords (per CSO-STD-0001).
Anti-Virus	
☐ Yes ☐ No	I have vendor supported anti-virus software installed and running.
☐ Yes ☐ No	My anti-virus software automatically updates itself.
☐ Yes ☐ No	My anti-virus software automatically scans my computer for viruses every day.
☐ Yes ☐ No	My anti-virus software automatically scans any IM (instant messaging) software I have installed on the computer.
Anti-Spyware	
☐ Yes ☐ No	I have vendor supported anti-spyware software installed and running.
☐ Yes ☐ No	My anti-spyware software automatically updates itself.
☐ Yes ☐ No	My anti-spyware software automatically scans my computer for spyware every day.
Email	
☐ Yes ☐ No	I agree to never open attachments unless I am expecting them.
☐ Yes ☐ No	I understand that malicious users frequently pretend to be a reputable company or individual and try to fool me into clicking on links within an email message that can install malicious code or direct me to their website for malicious purposes.
☐ Yes ☐ No	I agree to never open attachments that are programs (files that end with .bat, .chm, .cmd, .com, .exe, .hta, .ocx, .pif, .scr, .shs, .vbe, .vbs, or .wsf) from within the email message. I will save the file and scan it prior to opening it.
☐ Yes ☐ No	I agree to never respond to spam, even to "unsubscribe"
☐ Yes ☐ No	I understand that AOL, eBay, PayPal, my bank, and other Web sites related to my money will never send out requests for passwords, PINs, or other sensitive information via email, and I agree to never

NRC General User Remote Access Computer Security Checklist (Version 1.1)	
	click on links within these emails.
The Web	
☐ Yes ☐ No	I understand that advertisements on Web sites warning me that my computer can be hacked or fixed should be ignored and I agree that I will not click on those advertisements. I agree to seek guidance from the Computer Security Office regarding such possibilities and appropriate action.
☐ Yes ☐ No	I understand that web browsing can introduce malicious software onto my computer and thus place the NRC infrastructure at risk. I agree to configure my web browser to at least a medium-high security level to provide a minimum level of browsing security.
Personal Firewalls	
☐ Yes ☐ No	I have a personal firewall (e.g., Microsoft, Norton, McAfee) installed and running that is configured to protect against known malicious activities.
☐ Yes ☐ No	I understand when to allow software to access the Internet and when to be suspicious.
☐ Yes ☐ No	If there is a problem, I understand how to shut down all Internet activity using my personal firewall.
Wired or Wireless Router	
☐ Yes ☐ No	I have a wired router.
☐ Yes ☐ No	My wired router is configured according to NRC configuration requirements.
☐ Yes ☐ No	I have a wireless router.
☐ Yes ☐ No	My wireless router is configured according to NRC configuration requirements.
☐ Yes ☐ No	I changed all default passwords on my router(s) to be strong passwords.
☐ Yes ☐ No	I use strong passwords (per CSO-STD-0001) on all router accounts to which I have access.
☐ Yes ☐ No	I have ensured that I am using only a wired or wireless connection and that both a wired and wireless connection are not operating at the same time.

I attest to the correctness of the information on this checklist. If any conditions change, I agree to obtain a new approval prior to remotely accessing NRC computing equipment and networks.

Printed User Name	Signature	Date