Number	Blue box Display Message
	Theme: What is SCRM? (general awareness)
1.	Supply Chain Risk Management (SCRM) reduces supply chain vulnerabilities designed to exploit information systems.
2.	Supply Chain Risk Management (SCRM) provides for a secure safer online experience.
3.	People, Processes, and Technology are critical to securing the IT supply chain.
4.	A secure IT supply chain provides integrity to our classified and high unclassified systems.
5.	SCRM provides processes that if altered, interrupted, or halted could result in mission failure.
6.	SCRM mitigates vulnerabilities in information and communication technology products and services that are exploited.
7.	SCRM is inspecting critical products for evidence of unauthorized tampering and modification after repair.
8.	SCRM is implementing standardized practices that ensure products are not altered, or counterfeited.
9.	Product integrity means the delivered product operates free from deliberate or inadvertent manipulation.
10.	SCRM encourages best practices by the supplier to deliver services with necessary confidentiality, integrity, and availability.
11.	Identify and implement standards to promote process sustainability and reliability.
	Theme: How does SCRM impact the user?
12.	Supply Chain attacks can corrupt my system and create vulnerabilities that affect my work.
13.	Protection of all devices that connect to the internet is everyone's responsibility.
14.	Supply Chain security is a shared responsibility between acquirer, supplier, and user.
15.	Knowledge is power – understanding that there are threats in the supply chain is the first step in protecting yourself and DOE assets.
16.	Do you know where that thumb drive has been? Embedded malware is a common SCRM threat; protect yourself by scanning all external media at home and in the workplace.
17.	Have you received a promotional CD or thumb drive from a vendor lately? Be sure to scan all external media – even media provided as marketing material – to help mitigate supply chain threats.
	Theme: What is the Supply Chain Threat?
18.	Supply chain threats impact all users at home and work. Be vigilant to procure personal hardware and software from reputable vendors to help mitigate supply chain threats such as counterfeit or embedded malware.
19.	Supply Chain threats can cause catastrophic failures within our IT systems and components of our system.
20.	Counterfeit IT components create system vulnerabilities across the Federal IT space.
21.	The IT supply chain can be corrupted through the use of malicious code inserted into components prior to acceptance by DOE.
22.	Insider threat across the supply chain can produce components and systems that can

Number	Blue box Display Message
	cause mission failure.
	Theme: Cybersecurity/SCRM Messages
23.	Understand the supply chain threat and be vigilant as you access the network.
24.	When in doubt, throw it out! Don't open suspicious links in emails, tweets, posts, and ads.
25.	Protect *all* devices that connect to the Internet. Computers, phones, and games need protection from viruses & malware.
26.	The best defense against viruses and malware is to keep a 'clean machine.' Always install the latest upgrades (operating system, web browser, antivirus, etc.) and run virus scans regularly.
27.	USBs and other external devices can be infected by viruses and malware. Use your security software to scan them regularly.
28.	Many programs will automatically update to defend against known risks. Make sure your automatic update feature is turned on.
29.	All users have responsibilities from protecting DOE from the supply chain threat.
30.	Using the same external device in both a public computer and in a DOE network-connected computer introduces a considerable risk to the DOE computing infrastructure. Be vigilant as to where your external devices have been used and scan all external media regularly.
31.	Before you use the Internet, take time to understand the risks and learn how to spot potential problems.
32.	Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.
33.	Public computers are not secure! It is recommended that you not access or enter personal or sensitive information on a public computer.
34.	Connect with caution and be vigilant of potential threats