Visual Privacy: Under-Addressed Yet Critical Protection Area for the Federal Government

There is both a critical need and a basic expectation that the federal government will keep sensitive and classified information secure. Over the past few years, a wave of new federal security standards and increasingly sophisticated attacks have highlighted the need to protect sensitive and classified data at all times — while it is stored, transmitted and viewed. Much of this protection effort has been focused on two of those areas: data storage and transmission. This leaves a critical area, visual privacy — the protection of data that is displayed — under-addressed.

Some data security controls have been adopted widely by the federal government over the past few years: whole disk encryption for laptops and use of encrypted tunnels to transmit information (SSL, VPN, etc.). These technologies help protect data as it is stored and transmitted. However, there is still a risk of exposure whenever sensitive data is being displayed on a laptop, desktop monitor, or mobile device, as it should be protected from unauthorized viewing using controls like privacy filters. This visual protection is essential when working in a public place and in a trusted space with "need to know" information.

The explosion of mobile devices in government settings has increased the threat of a visual breach. President Obama, a longtime Blackberry user, continues to stay connected with his administration through a mobile device. Smartphones and other mobile devices, which access sensitive and classified information, have penetrated the highest levels of government. While significant time and energy is spent on securing the network infrastructure behind these devices and encrypting data on the device itself, it is also important to shield these devices from unauthorized view while in use.

The need to protect data from a visual breach has increased dramatically over the past few years. Consider the following:

- **Growing digitization of sensitive information:** Increasing demands for real-time access to decision-oriented information in the military, homeland security, medical responders, law enforcement, and other important governmental areas have accelerated the digitization of sensitive information. While efforts have been made to improve access controls for this information, the risk that a visual breach will occur as this information is displayed and used still exists.

Privacy and Compliance by the Federal Government:

Over the past decade, the federal government has drafted and adopted key standards to keep national secrets and its citizens' information secure. Protecting this data requires that security controls be in place as information is stored, transmitted and viewed. While there are a wide range of government standards that address data security and privacy, below is a summary of some key requirements:

Federal Information Security Management Act (FISMA): FISMA establishes a set of classification and protection guidelines for data managed by governmental agencies, government contractors, and related entities. FISMA has a number of supporting standards and guidelines which encourage agencies to take a holistic approach to data security.

NIST SP 800-53 "Recommended Security Controls for Federal Information Systems and Organizations"

The National Institute of Standards and Technology ("NIST") developed Special Publication 800-53 to outline a series of physical, technology and process controls for organizations under FISMA. As part of comprehensive security controls, section PE-5 requires that "the organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output."

- **Requirements to report data breaches:** Data breach notification laws have placed new requirements on agencies to notify an individual if they reasonably believe that his/her data was exposed to an unauthorized third party. Federal agencies routinely manage Personally Identifiable Information (PII) and Protected Health Information (PHI), and thus are susceptible to breaching notification laws enacted at the state level (in the case of PII). One avenue of data loss that must be defended is information displayed on the screens of federal employees and contractors.
- **Ease of screen capture:** The ability to inconspicuously capture information viewed on screens with camera phones has increased substantially. In fact, according to a recent survey, over 60% of US households now have at least one camera phone. This means that the use of a camera phone in a public setting to capture images — including images of other devices' screens — is much less conspicuous, thus making it much easier to gather information stealthily. This growth in access to technological advancements has made defending sensitive or classified information displayed on screens an essential component of data protection.

Adding security controls usually means reducing usability, performance and/or efficiency. In contrast, privacy filters help reduce risk continuously without burdening users. Further, they can give agencies more flexibility in where they position machines and how they allow employees to work outside of protected spaces.

Any comprehensive approach to safeguard data should include protecting that data while it is displayed on a screen. Attackers have shown innovation and resolve in their intelligence gathering activities. Classified information held by the federal government is a prime target. Adding privacy filters is a critical layer of defense to protect data from unauthorized insiders as well as external observers. Privacy filters, like those made by 3M, help block side views and can help government agencies and government contractors reduce the risk of exposing sensitive data they have been trusted with. 3M, a leader in privacy protection, offers a wide range of privacy filter products that are designed to protect laptops, desktops, mobile phones and other electronic devices.

For more information visit: **http://www.3Mscreens.com.**

Other standards and requirements: Beyond FISMA, numerous standards exist to protect data that is managed by the federal government. Depending on the type of data being managed, government agencies may fall under HIPAA (medical data), breach notification laws (Personally Identifiable Information), and several others. A common theme throughout these standards is the need for "due care" in handling sensitive information. An aspect of due care is ensuring visual privacy.

NIST SP 800-164 "Guidelines on Hardware-Rooted Security in Mobile Devices"

This guidance helps federal agencies mitigate three specific challenges with mobile devices, including device integrity, isolation and processes, and protecting storage.

56%
of Americans are smartphone owners.[1]

3Mscreens.com

[1]Smart Phone Ownership Reaches Critical Mass in the U.S., CNET, 2013.

Privacy is the best policy.

3M