

Keeping Sensitive Information Secure

*By Dick Cole
DCMA Public Affairs*

Identity theft is one of the fastest growing crimes in the country, and concern by the public is growing rapidly with each new data breach.

This increase in personal information being revealed to unauthorized individuals is a direct result of advances made in the area of computer technology and data collection that allow information sharing across agencies, governmental boundaries and service providers. As we are all aware from the news over the past few years, there have been a number of episodes of government agencies and corporations inadvertently divulging personally identifiable information.

PII is information that used to distinguish or trace an individual's identity, says Donna Williamson, the Defense Contract Management Agency's privacy officer. This includes such items as a person's name, Social Security number, or biometric records. These identifiers can either stand alone

or, when combined with other PII data, become linked to a specific individual, such as a date and place of birth or a mother's maiden name.

The Office of Management and Budget issued policy directives in 2006 requiring agencies to report *within an hour* even the suspicion of a data breach, Williamson says. This has helped raise the issue of data security to a top priority, moving agencies in the direction of strict accountability when it comes to the vulnerability of PII. In the past year, Williamson says DCMA has had 161 incidents involving the disclosure of PII.

If you even suspect the loss or compromise of PII, immediately report it to the privacy office. If you are uncertain whether an

inadvertent release or an actual compromise has occurred, Williamson advises that it is best to err on the side of caution and encourages employees to consult with her.

So what steps can we all take to avoid data breaches occurring within DCMA?

"At a minimum, minimize the amount of PII collected and only maintain what is strictly necessary to accomplish the mission," said Williamson. A good rule of thumb to follow is, "Don't collect personal data because it's always been done or because you might need it; collect it because you *need it*."

Several federal agencies inadvertently posted sensitive

Minimize the amount of PII collected and only maintain what is strictly necessary to accomplish the mission.

— Donna Williamson



Privacy officer Donna Williamson briefs Art Thurston, Fort Lee transition management office building manager, about protecting personally identifiable information. (Photo by Mark Woodbury, DCMA Public Affairs)

information to agency Web servers, according to Williamson. Policies governing the posting of PII, including access restrictions and permissions, must be carefully followed says Williamson. “It is a good idea to routinely check all content placed on Web sites,

shared drives and multi-access calendars for erroneous postings,” she says.

Most of the incidents in DCMA involve e-mails containing PII. Whether transmitted over the local network or beyond the network’s

security boundary, all e-mail containing PII must be encrypted. Williamson warns that if intended recipients do not have encryption capabilities, use another method of transmission, and if their certificates have not been set up, contact them to ask that they do so prior to transmitting the information. Another good practice is to announce that you are relaying PII. Additionally, when forwarding e-mails, unnecessary information should be dropped in e-mail threads, and when attaching documents, exercise caution to

Whether transmitted over the local network or beyond the network’s security boundary, all e-mail containing PII must be encrypted.

ensure unnecessary information is sanitized or extracted. Many employees have unknowingly forwarded e-mails with attachments containing PII, so be sure to check for hidden columns in spreadsheets.

“Another problematic area in the agency is the removal of PII from the workplace,” said Williamson, adding that “privacy data should never be removed from the workplace unless necessary to perform your official duty.” Williamson cautions that removal must be approved by your supervisor and warned that another problematic area is that well-intentioned employees are forwarding files containing PII to their home e-mail accounts to work from home, and this is never an acceptable practice.

DCMA is working to raise the level of awareness within the agency to prevent breaches of PII and has implemented computer

software to assist in preventing inadvertent disclosures. This tool monitors e-mail and Internet data on all DCMA computers. The tool checks incoming and outgoing data to ensure compliance with rules governing the transmission of Privacy Act information to ensure that such data is not transmitted without proper labeling or encryption. Violations result in real-time detection and flagging for action officer review to confirm the alert. If confirmed, the originator of the data, the originator’s supervisor and the DCMA privacy officer are advised of the incident and an appropriate report is sent to U.S. CERT — the U.S. Computer Emergency Response Team,” said Williamson.

In simple terms, this means that if you send an unencrypted e-mail containing PII, the software picks it

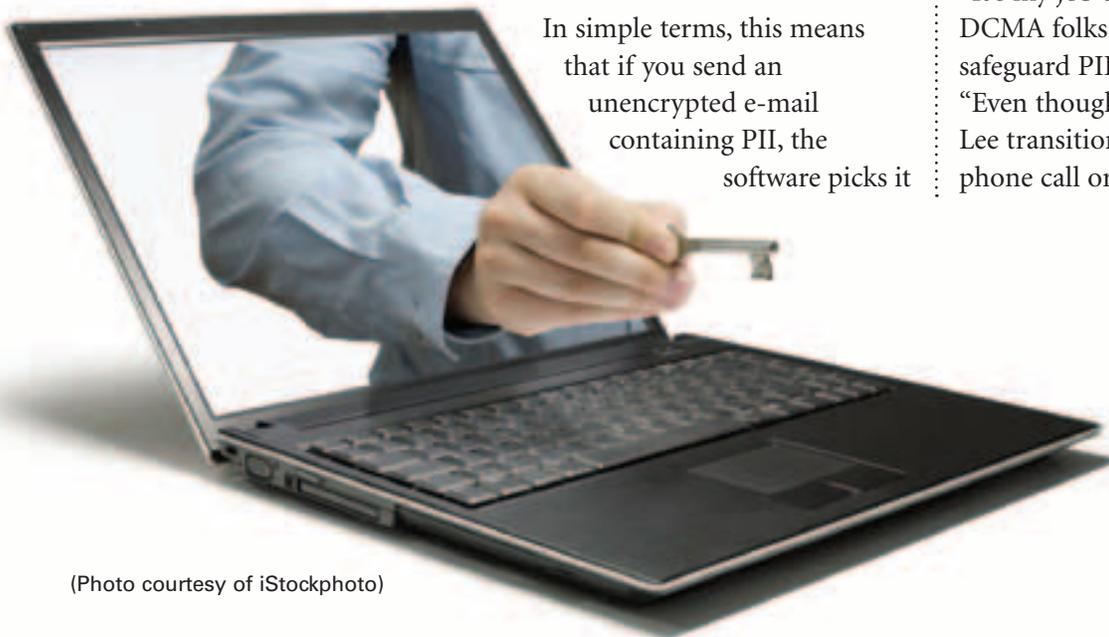
up and automatically notifies DCMA’s information technology customer support office, which files a report with US-CERT as required. ITSCO then sends an alert to Williamson, who will, in turn, contact the individual and his or her supervisor, as appropriate.

The best advice Williamson can give is to respect the privacy of others; take privacy protection seriously; alert your supervisor or other management official when you see personal data left unattended; report suspected privacy compromises to your privacy officer; know the Privacy Act requirements; and, above all, use common sense!

“It’s my job to be here to help DCMA folks know how to safeguard PII,” says Williamson. “Even though I’m down at the Fort Lee transition office, I’m only a phone call or an e-mail away.”

Privacy data should never be removed from the workplace unless necessary to perform your official duty.

— Donna Williamson



(Photo courtesy of iStockphoto)