

(U) 2012 Wisconsin National Guard Family Releasable Threat Assessment



**FORCE PROTECTION
BRANCH / PROVOST
MARSHAL OFFICE**

**JOINT FORCE
HEADQUARTERS-
WISCONSIN**



DEPARTMENT OF THE ARMY AND AIR FORCE
JOINT FORCE HEADQUARTERS WISCONSIN
WISCONSIN NATIONAL GUARD
2400 WRIGHT STREET
MADISON, WI 53708-8111

(U) FY 2012 Family Releasable Threat Information

Release: 1 May 2012

Contents

(U) SCOPE2

(U) KEY FINDINGS3

(U) THREAT MITIGATION AND RISK REDUCTION4

(U) DEFINITIONS6

(U) SCOPE

Although no specific credible threat has been identified; domestic law enforcement, intelligence agencies and antiterrorism proponents acknowledge there exists the potential for the activities or actions of certain groups to target members of the U.S. Military and their families, including the Wisconsin National Guard. The sources that might perpetrate these activities include criminal elements with larceny in mind, cyber criminals looking to exploit a financial weakness and possibly home grown violent extremists (HVE) looking to make a political or religious statement.

The Wisconsin National Guard is continuously monitoring classified and unclassified information pertaining to foreign and domestic threats. Some of the information monitored is of a general nature and non-specific to certain events or situations, and could serve to alert other citizens, specifically spouses, family members and dependents of Guard members to unusual events/occurrences. The Wisconsin National Guard leadership intends to share this type of information, when possible, with National Guard family members and dependents to increase vigilance, explain and reduce potential vulnerabilities and preclude the release of critical information.



(U) KEY FINDINGS

Wisconsin National Guard families can use the following information to protect their personal information, their families, as well as their military members. This is a brief list of types of adversaries, illegal acts they may perform, and how to protect them from these acts.

Adversary Type	Acts	Protection Measures
Criminals	Theft, breaking/entering, illegal drug activity, assaults, bullying, gang violence, workplace and domestic violence	Protect yourself from violent crime: http://www.ncpc.org/topics/violent-crime-and-personal-safety/protect-yourself-from-violent-crime What to teach kids about strangers: http://www.ncpc.org/topics/violent-crime-and-personal-safety/strangers
Cyber criminals	Phishing, vishing and smishing, identity theft, fraud, spear phishing	Install anti-virus and anti-spyware programs and keep them up to date. Install a firewall and keep it properly configured Regularly install updates for your computer's operating system Cyber security: Make it a Habit: http://www.dhs.gov/files/programs/gc_1202746448575.shtm Cyber security Tips: http://www.dhs.gov/files/events/cybersecurity-tips.shtm
Homegrown violent extremists (HVE)	Surveillance, elicitation/seeking information, tests of security, acquiring supplies, suspicious people who do not belong, dry run / trial run, deploying assets/getting into position, other	<p><i>"IF YOU SEE SOMETHING, SAY SOMETHING"</i></p> <p>Call 911 or your local police Submit a report to WiWatch: http://city.milwaukee.gov/wiwatch</p>
Terrorism		
<p>Additional websites of interest: An initiative of Wisconsin Emergency Management designed to educate and empower Wisconsinites to prepare for and respond to all kinds of emergencies including natural disasters and potential terrorist attacks. Readywisconsin.wi.gov</p> <p><i>Ready</i> is a national public service advertising (PSA) campaign designed to educate and empower Americans to prepare for and respond to emergencies including natural and man-made disasters. www.ready.gov</p>		

(U) THREAT MITIGATION AND RISK REDUCTION

LOSS OR THEFT OF IDENTIFICATION CREDENTIALS. Access to government facilities is usually based upon presentation of necessary access badges, keys and credentials needed to demonstrate a person's identity. Other uses of those credentials are to gain access to military facilities and automation systems. A lost or stolen electronic access key (EAK) could be used by an unauthorized person or adversary to gain access to a facility after duty hours as well as mis-representing a person attempting to gain access through an access control point to an installation or base. CAC cards are a little more problematic as they require a personal identification number (PIN) to access automation systems. The loss or theft of government personal identification items, i.e. ID cards, dependent I.D. cards, common access cards (CAC) and electronic access keys (EAKs) are critical events that must be reported to the chain of command immediately after the detection of loss or determination that they were stolen as a suspicious activity report.

LOSS OR THEFT OF MILITARY UNIFORMS. Similarly, as a lost or stolen identification card could be used to gain access to a facility, so could an unauthorized individual or adversary try to bluff their way into gaining access to a larger multi-unit, multi-service component facility based upon approaching in a stolen military uniform. The loss or theft of military uniforms or uniform related items are critical events that must be reported to the chain of command immediately after the detection and determination that they are either lost or stolen as a suspicious activity report. Service members should be vigilant to unfamiliar persons, who present themselves in incorrect uniform and be prepared to bring that situation to the attention of the chain of command. Unauthorized uniforms can also be easily purchased and impersonation of military personnel is becoming more common.



SUSPICIOUS PHONE CALLS AND IMPERSONATIONS. Recently there has been a proliferation of schemes seeking to exploit the family members and dependents of military service members, often when those military members have been deployed or are away for prolonged periods of training. The nexus of this group is that their targets are vulnerable and unable to easily validate the legitimacy of the offer(s) or statements that are being made to them. These mis-representations have varied from false death notifications to insurance/debt related matters to solicitations for funds to support the troops to false troop solicitation schemes. Family members who feel that they have been contacted by unidentifiable or suspicious sources should contact their service members unit of the Service Member Support Division at 1-800-292-9464 and select Option 3.

PROHIBITION ON COPYING MILITARY I.D. CARDS. All personnel and dependants are reminded that the photocopying of military identification cards and common access cards (CAC) is strictly prohibited. There have been recent incidents reported of commercial establishments photocopying U.S. government identification to verify military affiliation or provide government rates for service. These incidents are a violation of Title 18, U.S. Code, Part I, Chapter 33, Section 701 and are punishable by fine and/or imprisonment. Although commercial establishments may request to see military/ government identification, they may not photocopy or duplicate it in any way. Many military personnel and commercial establishments are unaware of the prohibition and the reasons it exists, which results in this being a fairly common practice. Because of the access the cards grant, criminal elements and terrorist organizations place obtaining U.S. government identifications at a premium when planning acts against the U.S. military. If a copied military or government identification fell into the wrong hands, it could spell disaster for the Armed Forces and the nation. Unfortunately, there are no safeguards in place to prevent a counterfeit military/government identification card from being produced based on a photocopy provided to a commercial establishment. For this reason, personnel are requested to remain vigilant

UNCLASSIFIED

in ensuring they do not allow anyone to photocopy their identification cards. The Provost Marshal recommends that all personnel, both military and civilian, provide a state drivers license or other form of photo identification to be photocopied when there is a request for such information by a commercial establishment. Further, that photocopying of those alternative documents should be done in the presence of the military member or dependant and it is recommended that unique data such as a date of birth and State Drivers License Numbers be redacted on the copy left with the merchant.

CYBER ISSUES. Two major concerns arise concerning the use of the Internet: 1) The unintentional release of information through social media sites and 2) the threat of identity theft through various on-line schemes both present challenges to service members and their family members and dependants.

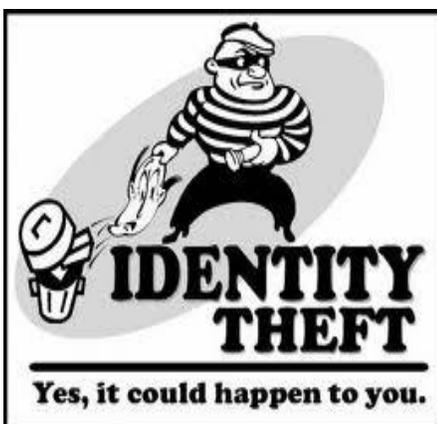
RELEASE OF INFORMATION THROUGH SOCIAL MEDIA. The Internet and social media has provided families with tremendous tools for staying in contact regardless geographic separations, but there is a downside to inadvertently releasing critical information that is accessible to others. It can make you, your family, or property a target for crime. Information contained in innocently intended messages and photographs can reveal close hold information concerning geographic coordinates, current preparations and future operations. Information about destinations, movement time and routes can be converted to intelligence data by our adversaries. Innocently transmitted digital photographs can contain geographic coordinates under a process known as "geo-tagging" unless that process is turned off on the camera before the picture is taken. Service members and their family members need to remain cognizant of the threat posed by providing certain information that could be exploited by intelligence operatives and criminal elements.



CYBER SCHEMES AND COMPROMISE OF PERSONAL IDENTIFICATION INFORMATION (PII). Whether for malicious or criminal intent, there are numerous means through which others may try to gain and exploit personal or financial information from service members and their families. Phishing is a form of social engineering attack using email or malicious websites to solicit personal information by posing as a trustworthy organization. The most common attacks come in the form of e-mails from recognizable companies, banks or organizations that tempt the reader to open a link. Phishing uses various techniques to trick users in to accessing the fake website, such as sending emails that pretend to be from a bank. These emails often use legitimate logos, a good business style and often spoof the reader of the email to make it look like it came from a legitimate bank. In general, these letters inform recipients that the bank has changed its IT infrastructure and asks all customers to re-confirm their user and identification information. When the recipient clicks on the link in

the email, they are directed to the fake website, where they are prompted to divulge their personal information. While most Internet users are familiar with the term phishing and its dangerous effects, security researchers are recording a considerable increase in two related malicious variations, vishing and smishing.

Although the concept of PII is old, it has become much more important as information technology and the Internet have made it easier to collect PII through breaches of internet security, network security, social networking, and web browser security - leading to a profitable market in collecting and reselling PII. PII can also be exploited by criminals to stalk or steal the identity of a person, or to plan a person's robbery and other crimes.



(U) DEFINITIONS

Click Jacking and Cross-Site Scripting - Click jacking and cross-site scripting are used to trick users into revealing confidential information, or taking control of a user's computer while they click on seemingly innocuous web pages. Users click on links they believe are valid links but are taken to a malicious website instead.

Hackers and Hacktivists - Hackers and hacktivists use loopholes or flaws in applications and Operating Systems or other programs to break into computer systems. Hackers are usually motivated by financial gains where hacktivists are usually motivated by political reasons.

Homegrown Violent Extremists/Terrorists - Be alert for these activities or signs of terrorism:

1. **Surveillance:** May include drawing diagrams, note taking, or vision-enhancing devices to monitor or record facilities and activities.
2. **Elicitation:** Attempts to obtain information on the people, procedures, or security of a facility.
3. **Tests of Security:** Attempts to breach security measures or assess response times.
4. **Acquiring supplies:** Gathering harmful chemicals, infected materials, or other supplies for attacks.
5. **Suspicious persons:** Person(s) who do not appear to belong in a given setting due to unusual behavior.
6. **Dry/trial runs:** Preparatory behaviors, such as practice runs or route mapping.
7. **Deploying assets:** Placing people and supplies into position to commit the attack.
8. **Other:** Incidents not fitting any of the above categories.

Malware – Malware, short for malicious software, is software that has been created for the purpose of doing harm. Malware includes viruses and spyware. A virus is a piece of code that is loaded into your computer against your knowledge. Viruses have different many different purposes some of which can be very harmful to the system or actively harvest PII, financial information, and passwords. Viruses are transmitted as attachments, downloads, visits to spoof and malicious websites, or through removable media such as USB drives or DVDs. Spyware are programs that typically run in the background to gather information about the computer or user.

Personally Identifiable Information (PII) - is information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Phishing (Spear Phishing) - Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit and steal personal information by posing as a trustworthy organization. The most common attacks come in the form of e-mails from recognizable companies, banks or organizations that tempt the reader to open a link. Phishing uses various techniques to trick users in to accessing the fake website, such as sending emails that pretend to be from a bank. These emails often use legitimate logos, a good business style and often spoof the header of the email to make it look like it came from a legitimate bank. In general, these letters inform recipients that the bank has changed its IT infrastructure and asks all customers to re-confirm their user information. When the recipient clicks on the link in the email, they are directed to the fake website, where they are prompted to divulge their personal information

Shoulder Surfing – Shoulder surfing refers to using observation techniques to get information. This can be accomplished by direct observation, use of closed circuit cameras, or binoculars. Perpetrators try to see PINs, passwords, or codes for ATMs, computers or lockers.