



20 Jun 2014

AFOSI SPECIAL PRODUCT



(U) United States: Safeguarding USAF Personnel's Online Presence



The unauthorized disclosure of classified information may be prosecuted under Section 793, Title 18, USC, and is punishable by fine of not more than \$10,000, imprisonment of not more than 10 years, or both.

(U) Safeguarding USAF Personnel's Online Presence

(U) INFORMATION CUTOFF DATE: 16 June 2014

(U) PREDICATION:

(U//FOUO) This Air Force Office of Special Investigations (AFOSI) Investigations, Collections, and Operations Nexus (ICON) product examines how to protect United States Air Force (USAF) personnel from impersonations, fraud, and possible adversarial foreign agencies online. The intended audience for this product is USAF military members, civilians, and families of USAF employees. This product contains CONTROLLED UNCLASSIFIED information derived from: AFOSI investigative files; AFOSI localized criminal threat assessments; international, federal, state, and local law enforcement sources; and other applicable open-source information. Source documents and analysis within this document were limited to reporting classified at the UNCLASSIFIED//FOR OFFICIAL USE ONLY level or lower.

(U) EXECUTIVE SUMMARY:

(U//FOUO) Malicious use of personal information posted on the Internet is frequently utilized by nefarious actors for two major purposes: fraud and solicitation. Online fraud against USAF personnel has persisted for many years and can take on multiple forms, including romance scams, online sale scams, or advance-fee scams. Solicitation of USAF personnel by possible foreign adversaries is a growing concern for AFOSI, especially on social networking sites such as Facebook and LinkedIn.

(U) Fraudulent online activities involve a wide variety of sophisticated scams and fraud schemes designed to take advantage of the unsuspecting public. Scammers use actual and fictitious information about DoD members in a variety of Internet ploys designed to extort information or money from victims. Even high-ranking Department of Defense (DoD) officials and general officers (GOs) have not been immune to these online schemes, as perpetrators use their identities and photographs to lure and defraud victims. DoD members are particularly susceptible to online impersonation based on their elevated social status and perceived integrity. DoD members' institutional and social stature provides cybercriminals with the reputability and plausibility necessary to make these online scams appear credible; hence, DoD members appear to be attractive targets for Internet imposters because of their personal reputation and the reputation of the institution of which they are part.

(U//FOUO) Fictitious online profiles controlled by foreign adversaries have successfully targeted hundreds of DoD members, including USAF personnel. These malicious actors typically create fake profiles on social networking sites with legitimate-looking information and attempt to send "friend" or "connection" requests to unsuspecting victims. Similar to criminal actors, foreign adversaries use photographs and career

information posted by actual DoD personnel on social networking sites to create fictitious profiles in order to further entice a victim. Once connected, these malicious actors often attempt to either solicit sensitive information about a victim's career or send private messages with malicious links. DoD members are high-value targets because of their perceived connections to sensitive military programs, such as Remotely Piloted Aircraft (RPA) and nuclear weapons.

(U) Since the mere act of online impersonation alone may not constitute a crime, law enforcement authority is limited. AFOSI and law enforcement agencies at all levels have difficulties investigating online impersonations and fraud-based Internet crimes for the following reasons: (1) Internet scams often traverse international boundaries of countries that limit successful investigations. (2) the online scams traverse untraceable computer systems (3) the financial loss may not meet the threshold to justify investigations, (4) military investigative agencies, such as AFOSI, are often limited in their jurisdiction to investigate matters of online impersonations when the subjects behind the criminal acts, nor the victims who have been scammed out of money, goods, or services, are DoD members.

(U) DoD members should remain vigilant against these types of online activities by reducing their online footprint and reporting any improprieties regarding their personal information or suspicious "connection" requests to appropriate authorities. The fastest, most direct way to remove fraudulent information is for the impersonated member to contact the social networking site where the offense occurred. Typically, impersonations are in violation of the provider's terms of service and the fraudulent profile will be removed. **Appendix 1** includes instructions on how to remove impersonating information from the most popular social media websites. **Appendix 2** includes contact information for many online social media providers.

(U) KEY JUDGEMENTS

(U) Criminals will continue, into the foreseeable future, to utilize DoD personnel information to target susceptible victims for multiple online fraud schemes, including relationship scams, online sale scams, and advance-fee scams due to DoD member's perceived integrity and elevated social status. AFOSI assesses this with *high confidence* due to the amount of reported impersonations and fraudulent accounts provided to AFOSI.

(U//FOUO) DoD members, including USAF, are high-value targets for possible foreign actors seeking information on sensitive programs such as Remotely Piloted Aircraft (RPA) and nuclear weapons technology. Therefore, foreign actors will likely continue targeting DoD members and civilians utilizing social networking sites. AFOSI assesses this with *high confidence* due to recent open-source reports detailing possible malicious Iranian activity targeting DoD members on social media sites.

(U) FRAUD TARGETING USAF MEMBERS

(U) The Internet Crime Complaint Center (IC3) has warned that online fraudsters are increasingly impersonating DoD personnel online in order to deceive potential victims.¹ IC3 is a task force established jointly by the Federal Bureau of Investigation and the National White Collar Crime Center, with the aim of tracking cybercrime activities, generating leads for law enforcement agencies, publishing public service announcements and intelligence reports. According to IC3, online scammers use DoD members' information, whether real or fake, for three reasons: (1) credibility, (2) plausibility, and (3) emotional appeal.² By appealing to victim's sensibilities, the criminal establishes trust and loyalty in order to boost credibility once the scam is proposed. The DoD nexus also gives criminals a credible reason to solicit money from victims that would otherwise make such a request seem suspicious. For instance, a criminal may ask a victim for money in order to fund "visa documents" so that the criminal can "come home from deployment."

(U) Those who are impersonated online are generally not the victim of criminal activity. The victim is the person scammed out of money, goods, or services and is incurring a loss. While those impersonated may encounter damage to their reputation due to their name's affiliation to the Internet scam, they are not victims of criminal activity.

(U) Figure 1: Scammers Using Same Public DoD Photo for Multiple Profiles ³



(U) Types of Scams

(U//FOUO) Recent years have been marked by an increase in online scams involving DoD imposters as cybercriminals look to exploit the public's confidence in the U.S. armed services. In September 2011, *Army Times* highlighted the extent of the problem when it published an article claiming that the United States Army has seen an explosion of cases that Internet scammers adopt identities of soldiers at all levels.⁴ In fact, the United States Army Criminal Investigations Command received nearly 100 complaints involving the online impersonation of Army personnel, 29 of which were high-ranking Army officials.⁵ Other armed services, including the USAF, are also encountering cases where members have been subjected to online impersonation regardless of rank, thereby confirming that perpetrators are targeting DoD members across services and ranks.

(U) Although there are a variety of online scams, the following are the most prevalent online impersonation schemes involving U.S. service members:

(U) **Trust-based online relationship scams:** Trust-based scams online seek to defraud potential victims by pretending to be service members seeking romance or who are in need of emotional companionship. In such scams, cybercriminals often derive information for their fictionalized DoD characters from official DoD websites and social networking websites where DoD families post information about their loved ones.⁶ They gather enough detailed personal information (including pictures) to lure unsuspecting victims (most often women) into sending money to help them with transportation costs, marriage processing, medical fees, communication fees (laptops and satellite telephones) or other concocted stories tailored to appeal to victims' emotions.^{7 8} Perpetrators in these cases typically promise that they will repay the victim when they finally meet; however, once the victim sends the money the scammer is never heard from again.

(U) **Online sale scams:** Online sale scams are designed to lure potential victims into the scam by offering online goods well below their market price, most frequently carried out on eBay, Yahoo! Autos, or Craigslist. Most of these scams involve vehicle sales and generally take the following pattern: a scammer advertises a vehicle for sale at a price that is almost too good to be true. He/she describes the vehicle in broad terms, such as: "It has a clean title, very well maintained, always garage kept, no rust, excellent condition, runs and sounds 100% perfect with no leaks or noises."⁹ The potential victim answers the ad and is soon contacted by the scammer, claiming to be a service member with a U.S. military unit¹⁰ that is being deployed abroad. The scammer uses his "deployment" to explain the undervalued sales price of the vehicle and the fact that the potential victim will be unable to test drive it. Often, the scammer insists that the transaction take place quickly and requests that the potential victim wire the money (usually via Western Union and MoneyGram) to the scammer.

(U) **Advance-fee online fraud scam or Nigerian Letter scams**¹¹: Advance-fee scams seek to defraud potential victims by promising big profits in exchange for help moving large sums of money. Claiming to be

a government/DoD official, business/DoD person or the surviving spouse of a former government leader, perpetrators offer to transfer millions of dollars into victim's bank account in exchange for a small fee. Some utilize photographs and biographical information of high-profile US DoD officials obtained from the Internet in e-mails or on social/dating sites to extort money from unsuspecting citizens.

(U//FOUO) Possible Foreign Adversaries Targeting DoD Personnel

(U//FOUO) According to a report by a U.S. Security Company, foreign adversaries have targeted over 2,000 people using false personas on multiple social networking sites.¹² These actors have primarily targeted mid to high-level victims associated with cleared defense contractors (CDC) and DoD. Many of these personas are linked to the fictitious news agency, NewsOnAir.org, which reposts news articles from legitimate sources, such as the Associated Press and Reuters, and then claims it produced the articles themselves. According to the U.S. Security Company report, the ultimate sponsor of the activity is unknown; however, indications suggest it originates from Iran.¹³

(U//FOUO) Foreign actors may be interested in targeting USAF personnel because of the sensitivities of DoD work environments and technologies that are currently employed by the USAF. DoD and USAF personnel may be particularly susceptible because of the generally held belief that having a sprawling presence on professional social networking sites, such as LinkedIn, are beneficial to one's career. Many CDCs and associations that work closely with the USAF have their own groups on social networking sites that are open for anyone to join. Many of these groups have thousands of members affiliated with units across the DoD. These groups allow a foreign adversary seeking a target the ability to freely comb through thousands of profiles without directly connecting to the victim.

Figure 2: (U) Example of Fake Profile¹⁴



(U) Incidents of Online Impersonation Involving US DoD Members

(U) One of the best examples of how susceptible the public is to online DoD impersonation was demonstrated in 2010 when a security researcher created a fake LinkedIn account under the name Robin Sage. The researcher built a prestigious resume for Robin Sage: a degree from MIT, an internship at the National Security Agency, and a current position at the Naval Network Warfare Command (Figure 2). Her address was that of BlackWater, a military contractor. In addition, the researcher included an attractive photograph of a random woman in the profile. Robin Sage gained a total of about 300 friends on LinkedIn. Among the connections were senior DoD and Intelligence Community officials, as well as several other DoD and military personnel.¹⁵ The Robin Sage incident highlights how easy it can be to trick even high-level service members into providing personal information to unknown actors.

Figure 3: (U) Robin Sage's LinkedIn Profile ¹⁶

Robin Sage you

N8 at NETWARCOM

Norfolk, Virginia Area | Computer & Network Security

Current

- **N8 at Naval Network Warfare Command**

Past

- Intern at Government Agency

Education

- Massachusetts Institute of Technology
- St. Paul's School

Recommendations 1 person has recommended Robin

Connections 147 connections

Websites

- Where I Work
- Dark Side of Security
- My Facebook

Twitter

- robinsage

Public Profile <http://www.linkedin.com/in/robinsage>

Summary

I have been in the computer hacking scene for over ten years. During this time I have penetrated hundreds of networks as a professionally contracted hacker and was empowered by the adrenaline rush of breaking into secured facilities of Global 500 companies and various governments. Because of my style and diverse areas of expertise, many of my friends refer to me as the real life Abby Scuito of NCIS.

(U) Apart from the Robin Sage incident, the following is a sample of additional instances where cybercriminals assumed the identities of high ranking DoD members, including GOs, in an attempt to scam unwitting victims:

- (U//FOUO) In mid-2014, a civilian informed AFOSI that they were contacted on Skype by a man claiming to be a Brigadier General. The scammer used a picture of the Brigadier General taken from a public USAF website in his Skype profile. The victim claimed that the scammer had a heavy accent and may have been attempting to conduct a romance scam.¹⁷
- (U//FOUO) In early 2014, a scammer utilized the public information of a Lieutenant General in a romance scam against an unsuspecting victim via e-mail. After multiple exchanges, the scammer asked the victim for money.¹⁸
- (U//FOUO) An unknown scammer had utilized the persona of a high-level USAF officer since at least 2011 and as recent as 2013 to conduct multiple fraud attempts against various victims, typically unsuspecting females.¹⁹
- (U) In 2011, a scammer used a high-ranking USAF officer's biographical information posted on an AF website in an effort to perpetrate an advance-fee online fraud scam. The imposter, claiming to be engaged in a multi-million dollar transfer of Iraqi funds on behalf of U.S. government, attempted to extort personal information from unwitting victims. To further lend credibility to his scam, the perpetrator hyperlinked to the Air Force's news story depicting the GO's activities in Iraq and interaction with high-level Iraqi military officials.²⁰
- (U//FOUO) In 2010, a cybercriminal assumed the identity of a USAF GO in an effort to perpetrate online romance scam. Using a high-ranking USAF officer's public online information (photograph, name, and bio information), the perpetrator created fake social networking profiles (Facebook, MySpace and Zoosk) that were used to interact with potential victims. One female victim was deprived of \$10,960.²¹

(U) Scammers utilizing military information often exhibit obvious signs that the profile is fake, including:

- (U) **Lots of "friends" or "connections" added in a short amount of time:** Scammers want to acquire as many contacts as possible to help bolster the legitimacy of their profile.
- (U) **Inconsistencies in profile information, such as suspicious employer or education information:** Scammers will often misspell employers and school names, or may include generic profile information, such as only writing "college" for where they attended school.

- **(U) Very little profile interaction:** Profiles may include very few or generic comments from the scammer, such as an occasional, “Thanks for the add”.
- **(U) Multiple grammatical errors and spelling mistakes:** Many scammers are not native English speakers and will often phrase information incorrectly or will not capitalize proper nouns, such as their own profile name.
- **(U) Very few real photos:** Scammers will often tag themselves only in cartoons or celebrity photos frequently found on the Internet.
- **(U) Friends are rarely located in the same area:** Since scammers want to connect to as many people as possible, they will spam thousands of users all over the world with “friend” requests; scammers often have very few connections within a local area.

Figure 4: (U) Example of Fake Profile Using Military Information ²²



(U) LIMITATIONS OF LAW ENFORCEMENT AUTHORITIES

(U) The mere act of online impersonation is not a crime absent of overt acts by the impersonator to use the information to scam a victim out of money, goods, or services. Members who believe they are a victim of Internet crime where a financial loss exists should report the criminal activity to local law enforcement. Law Enforcement authorities, including AFOSI, will assess the situation to determine if an investigation is a feasible option, and work to ensure the matters are referred to the appropriate agency. AFOSI and law enforcement agencies at all levels have difficulties investigating online impersonations and fraud based Internet crimes for the following reasons: (1) Internet scams often traverse international boundaries of countries which may not cooperate with US authorities or lack the laws or means to support international investigations. (2) Criminals committing these scams often utilize untraceable computer systems, routing accounts through numerous locations around the world. (3) Internet scams often do not meet financial threshold which justify the costs or efforts associated with international investigations, or the matters do not meet the threshold for prosecution. According to IC3 statistics, of the 115,903 Internet criminal complaints reported involving a financial loss in 2011, the average loss was \$4,187; well below the threshold required for investigators to obtain court ordered warrants and subpoenas.²³ (4) Military investigative agencies, such as AFOSI, are often limited in their jurisdiction to investigate matters of online impersonations when the subjects behind the criminal acts, nor the victims who have been scammed out of money, goods, or services, are military members.

(U) PREVENTION AND MITIGATION

(U) Although refraining from posting personal information or pictures on public websites is generally the best defense against online impersonators, this is often neither possible nor practical. Nonetheless, US Service members can take proactive measures to reduce their online footprint and mitigate potential risks to their personal information. Outlined below are several measures designed to safeguard personally identifiable information and reduce online presence, along with a list of relevant authorities that victims can turn to in case of online impersonation.^{24 25}

(U) Limit Your Exposure and Use Caution

- **(U) Only reveal what you would feel comfortable revealing in a public setting** - Use extreme diligence and assume no privacy when posting new information. If a website requires a phone number or e-mail address for registration, utilize free services such as Gmail, Hotmail, and Google Voice, to create “throwaway” accounts for the purpose of registering.
- **(U) Lock down privacy, access, searching, and sharing settings** - The most popular social networking sites have options for limited the exposure of your personal information only to “connections” or “friends” that are explicitly approved by the account owner.

- **(U) Disable features that automatically broadcasts or tags a photo with your current location** - Cell phones often integrate social media apps directly into the built-in camera application. When a photo is taken, some social media apps will automatically determine your current location and upload that data to your social networking site for all to see.
- **(U) Disable automated GPS and location tracking features when not in use** - Many map and navigations apps on cell phones, tablets, and PCs will continue to collect information about your whereabouts even when you are not actively using them. Carefully scrutinize any applications settings used on mobile devices or home computers as they can be used to determine patterns of life or perhaps tip off your location if used.
- **(U) Do not reveal mission-related information** - Do not post sensitive information related to your unit, deployment, activities, or operations tempo, and request that friends and family do the same.
- **(U) Use discretion when accepting new “friends” or “connections”** - Be wary of accepting invites from names you either vaguely or don't know and always check directly with a contact before accepting seemingly legitimate requests to join networks or sites.
- **(U) Limit the personal information you post online** - If possible, do not post your full name, birth date, school information, or work history.
- **(U) Do not post relationship statuses between you and your significant other, children, or family members** - Such information could be used for targeting purposes by possible criminal and malicious foreign actors.
- **(U) Do not tag identifiable pictures of yourself online** - If others have posted pictures of you, un-tag yourself. This information could be used to create impersonating profiles or used for targeting purposes.
- **(U) Permanently deleting your profile is ultimately the best way to prevent information from being collected on you, your friends, and your family.**

(U) Aggregators: Opt Out of Services or Remove the Source of Information

- **(U) Opt out of services of aggregators by visiting their sites and officially requesting that information be removed** - Data aggregators, such as spokeo.com, intelius.com, and 123people.com, collect information on individuals from hundreds of public databases and

collates the data onto their website for customers to purchase. This can be done legally without the permission of the individual whose data is collected. Even if a person opts-out of inclusion into the website's data aggregator, the permission will be reset once the person moves to a new address. Individuals should frequently search for themselves and their families on these websites and opt-out as soon as possible after a move.

- **(U) Remove or limit personal information, such as e-mail addresses, phone numbers, etc., on websites that are searched by aggregators** - In addition to public records, data aggregators collect information from websites associated with social media, online gaming, internet forums, gambling, and hundreds of others. Users should use caution when registering for a website.

(U) Specific Recommendations for Popular Websites

- **(U) Facebook:** Make sure your privacy settings are set to the maximum level where only you can view your own personal information. Often re-check your privacy settings because Facebook constantly changes many of its privacy features.
- **(U) LinkedIn:** Make sure your job description does not include sensitive information that could be used for identification or targeting purposes. Disable showing your groups and connections to people searching for you. Limit your profile only to your 1st level connections.
- **(U) MySpace:** Change your privacy settings so that your full profile is only visible to friends.
- **(U) White Pages:** Search for your name or phone number. Click on your profile and then find the tab labeled, "Claim/Edit". Click this tab and then click the "Login" link. Click the link, "Not interested in using Facebook?" (It is highly recommended that you **DO NOT** use your Facebook account to create a new profile). On the next page, click "Create an account". Enter your information along with a non-DoD associated e-mail address. After you log-in, click on "My Account" in the top-right corner and then select "Account". Under the "Privacy Settings" area, click on "Show Information". Check the box marked, "Hide all information about me" and confirm.
- **(U) Public aggregator websites, such as spokeo.com, pipl.com, zabasearch.com, radaris.com, and 123people.com:** Most data aggregators allow you to opt-out of their public indexing searches by sending an e-mail to the company or filling out a form. Other sites, such as intelius.com, require you to e-mail or fax them a copy of your driver's license in order to remove your profile. Typically, this is safe to do, but make sure you upload the scanned license to the real website.

- **(U) Webmail services, such as Gmail, Hotmail and Yahoo!:** Many free e-mail services will often create a publically searchable profile with the information entered during e-mail creation. Check privacy settings on any e-mail accounts to verify personally identifiable information is not public.

(U) What To Do If You Have Been Impersonated Online

(U) Once your identity has been impersonated, action needs to be taken by you to prevent further/possible criminal activity. The following actions should be taken immediately:

- **(U)** If it is known that your impersonated information has been used to scam victims out of money, goods or services, please report the activity to local law enforcement immediately.
- **(U) Report the fraudulent account to the website where it is hosted.** This is the fastest and most direct way to remove the impersonating account. For example, if the impersonating account is on Facebook, contact Facebook directly. See Appendix 1 for removal information for the most popular websites used for impersonation. *Please note: Companies often change their procedures for fraudulent account removal.* If removal instructions in Appendix 1 do not work, review the website's terms of service and/or use a search engine to find the latest instructions. For example, to find the latest Facebook removal instructions, use a search engine such as Google and search for "report Facebook impersonation" (without quotes). Be sure to check that the link you click on after the search directs you to the official Facebook website.
- **(U) Conduct an online search and remove publically available information.** Often, criminals will use the same impersonated information on multiple social networking or dating websites.
- **(U) Report the incident to the Internet Crime Complaint Center (IC3) (FBI-NW3C Partnership).** The victims of Internet crimes should report the impersonation and related activity to the IC3 website at: <http://www.ic3.gov/>. Please describe in detail as much as you can about the impersonation, including if you know that the account was used for scamming victims out of money. The IC3 will include the impersonation and other Internet crimes in its statistics and refer the complaint to appropriate authorities if further investigation is possible.

(U) CONCLUSION

(U//FOUO) USAF personnel appear to be susceptible to online impersonation because of the perceived reputability and integrity of Service members by the general public. Criminals and possible foreign intelligence entities (FIE) looking to impersonate Service members can find an abundance of personal information from official DoD websites, news articles, and social networking sites, especially on GOs and high-ranking DoD officials. USAF members should be aware that their personal information can be exploited by online imposters and must remain vigilant to protect and minimize their Internet footprint.

(U) ADMINISTRATIVE INFORMATION

(U) Author: AFOSI ICON/Cyber Integration Desk, afosiicon-cyberdesk@us.af.mil, 571.305.8525

(U) Reviewed by: AFOSI ICON/Cyber Integration Desk, Senior Analyst, afosiicon-cyberdesk@us.af.mil, 571.305.8540

(U) This product was coordinated with: N/A

(U) AFOSI Analysis Products are available at www.afosi.af.smil.mil (SIPRNet) and www.afosi.ic.gov (INTELINK-SCI)

(U) Product Number: 14937

(U) Please provide feedback, comments, or suggestions to afosiicon-productionmanagement@us.af.mil.

(U) Source Summary Statement:

(U) Original sources of the information contained in this report include reports from The Internet Crime Complaint Center's (IC3) periodic Trend Analysis and Intelligence Brief; AFOSI criminal investigative reports; media and news accounts of online social networking incidents involving service members; and, Army Criminal Investigation Command (Army CID). The information for this product was derived from AFOSI systems and open source reporting on global, cyber-criminal activity. AFOSI judges the assessments and judgments in this product to be accurate based on past precedence and the quantity and quality of reporting on this subject matter.

(Intentionally Left Blank)

(U) CONFIDENCE LEVELS & ESTIMATIVE LANGUAGE

(U//FOUO) Estimative Language

(U) Confidence Levels

<p>Low</p> <p>Little or no information available, intelligence from untested sources, or for which there is little or no corroboration. Low confidence generally means that the information is scant, questionable, or very fragmented; that it is difficult to make solid analytic inferences; or that AFOSI has significant concerns or problems with the sources.</p>	<p>Moderate</p> <p>Indirect or derived intelligence from multiple sources or from a single reliable source. Moderate confidence generally means that the information is interpreted in various ways, that AFOSI has alternate views, or that the information is fragmentary and/or not sufficiently credible and plausible to render a solid judgment.</p>	<p>High</p> <p>Direct or high-quality intelligence from multiple sources or from a single highly reliable source, such as high-quality imagery, human intelligence, or signals intelligence. High confidence generally indicates that AFOSI's judgments are based on high quality information or that the nature of the issue makes it possible to render a solid judgment.</p>
---	---	--

(U) Estimates of Likelihood

Very Unlikely	Improbable	Even Chance	Probable	Very Likely Almost Certainly
0 - 10%	10% - 40%	40% - 60%	60% - 90%	90% +

(U//FOUO) AFOSI uses the IC estimative language standard. Phrases such as “we judge,” “we assess,” and “we estimate,” as well as terms such as “likely” or “possible” represent AFOSI’s effort to convey a particular analytical assessment or judgment. Such terms do not constitute fact, proof, or knowledge and may be based on incomplete or fragmentary information. Some analytical judgments are based directly on collected information; others are based on historical judgments and past analytical assessments. “Might” and “may” reflect situations where AFOSI is unable to assess likelihood, generally because relevant information is unavailable, questionably sourced, or fragmentary. Intelligence judgments pertaining to “likelihood” are intended to reflect the approximate level of probability of a development, event, or trend. Assigning precise numerical ratings to such judgments would imply more rigor than the agency intends.

(U) REFERENCES

- ¹ (U) IC3; **The Internet Crime Complaint Center’s (IC3) September 2011 Trend Analysis and Intelligence Brief**; “Government Officials’ Identity Being Used on Social Networking Sites”; Sep 2011; Overall classification is **UNCLASSIFIED**
- ² (U) AFOSI; **CIR 10-03**; Online Criminals Posing as U.S. Military Personnel, Air Force Office of Special Investigation; Dec 2010; Overall classification is **UNCLASSIFIED//FOR OFFICIAL USE ONLY**
- ³ (U) US Army Public Affairs; **“Army stresses caution, education to combat social media scammers”**; 11 July 2011; <http://www.army.mil/article/61432/>; Overall classification is **UNCLASSIFIED**
- ⁴ (U) Army Times; **“Army expands warnings on social networking”**; 26 September 2011; <http://www.armytimes.com/article/20110926/NEWS/109260312/Army-expands-warnings-social-networking/>; Overall classification is **UNCLASSIFIED**
- ⁵ (U) Army CID; **Author Interview with the USACID Computer Crimes Program Manager**; 20 June 2012; Overall classification is **UNCLASSIFIED//FOR OFFICIAL USE ONLY**
- ⁶ (U) Marine Corps Times; **“Online Colonel Seemed Like a Catch”**; 30 December 2007; <http://www.marinecorpstimes.com/article/20071230/NEWS/712300301/Online-colonel-seemed-like-catch/>; Overall classification is **UNCLASSIFIED**

- ⁷ (U) Executive Gov; “**Army Impersonators Scam Women on Dating, Social-Networking Sites**”; 24 March 2010; <http://www.executivegov.com/2010/03/army-impersonators-scam-women-on-dating-social-networking-sites/>; Overall classification is **UNCLASSIFIED**
- ⁸ (U) TS2; “**TS2 Warns of Fraudulent Satellite Offers**”, Undated; www.ts2.pl/en/Scam-Warning; Overall classification is **UNCLASSIFIED**
- ⁹ (U) Syracuse Post-Standard; “**Con Artists Pretend to be Soldiers in Car Selling Scam**”; 2 November 2008; http://www.syracuse.com/news/index.ssf/2008/11/con_artists_pretend_to_be_sold.html; Overall classification is **UNCLASSIFIED**
- ¹⁰ Ibid.
- ¹¹ (U) Army CID; “**Nigerian and Impersonation Fraud Response Letter**”; Undated; Overall classification is **UNCLASSIFIED**
- ¹² (U) iSight Partners, “**NEWSCASTER: An Iranian Threat Within Social Networks**”; Pg. 3; 28 Mar 2014; Overall classification is **UNCLASSIFIED**
- ¹³ (U) iSight Partners, “**NEWSCASTER: An Iranian Threat Within Social Networks**”; Pgs. 10-11; 28 Mar 2014; Overall classification is **UNCLASSIFIED**
- ¹⁴ (U) PC World; “**Taliban uses sexy Facebook profiles to lure troops into giving away military secrets**”; 11 Sep 2012; Overall classification is **UNCLASSIFIED**
- ¹⁵ (U) Dark Reading Security; “**Robin Sage Profile Duped Military Intelligence, IT Security Pros**”, Dark Reading Security; 10 July 2010; <http://www.darkreading.com/risk/robin-sage-profile-duped-military-intelligence-it-security-pros-/d/d-id/1133926>; Overall classification is **UNCLASSIFIED**
- ¹⁶ (U) Computer World; “**Fake femme fatale shows social networking risks**”; 22 July 2010; http://www.computerworld.com/s/article/9179507/Fake_i_femme_fatale_i_shows_social_network_risks; Overall classification is **UNCLASSIFIED**
- ¹⁷ (U) AFOSI; **I2MS Case # 33892141361519**; Accessed 18 June 2014; Overall classification is **UNCLASSIFIED//FOR OFFICIAL USE ONLY**
- ¹⁸ (U) AFOSI; **I2MS Case # 32867140291209**; Accessed 18 June 2014; Overall classification is **UNCLASSIFIED//FOR OFFICIAL USE ONLY**
- ¹⁹ (U) AFOSI; **I2MS Case # 28815131462124**; Accessed 18 June 2014; Overall classification is **UNCLASSIFIED//FOR OFFICIAL USE ONLY**
- ²⁰ (U) Scam of the Day, “**8 November 2011**”; www.scamoftheday.com; Overall classification is **UNCLASSIFIED**
- ²¹ (U) AFOSI; **I2MS Case # 32714103432303**; Accessed 18 June 2014; Overall classification is **UNCLASSIFIED//FOR OFFICIAL USE ONLY**
- ²² (U) Associated Press; “**Soldier impersonations target women on Facebook**”; 27 February 2011; <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/27/AR2011022700792.html>; Overall classification is **UNCLASSIFIED**
- ²³ (U) IC3; **The Internet Crime Complaint Center’s (IC3) September 2011 Trend Analysis and Intelligence Brief**; “**Government Officials’ Identity Being Used on Social Networking Sites**”; Sep 2011; Overall classification is **UNCLASSIFIED**
- ²⁴ (U) AFOSI; “**Guidance on Reducing USAF Members’ Internet Footprints and Protecting Online Information**”; 22 July 2011; Overall classification is **UNCLASSIFIED//FOR OFFICIAL USE ONLY**
- ²⁵ (U) AFOSI; “**Removing Impersonating Accounts on Social Network Sites**”; 8 September 2011; Overall classification is **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U) APPENDIX 1
(U) Removal Instructions for Popular Websites

(U) FACEBOOK

(U) If you **DO** have a Facebook account:

1. Visit the impersonating account's Facebook page / timeline
2. Click the ●●● and then select "Report"
3. Click "Report this account"
4. Click "This person is pretending to be me or someone I know"
5. Complete to on-screen directions and submit
6. Allow 5 business days for Facebook to contact you or remove the profile

(U) If you **DO NOT** have a Facebook account:

1. Visit: <http://www.facebook.com/help/contact/?id=169486816475808>
2. Fully complete the form, including providing a scanned government-issued ID of the impersonated person
3. Allow 5 business days for Facebook to contact you or remove the profile

(U) HOTMAIL / OUTLOOK.COM / LIVE.COM

1. E-mail abuse@live.com with information about the impersonating account. Include as much information about the impersonating account as needed. Explain who you are and attach the screenshot as evidence
2. Allow 5 business days for Hotmail to reply to your e-mail
3. Follow the steps outlined in Hotmail's response

(U) LINKEDIN

1. Take a "screenshot" of the impersonating account. To complete this, press "Print Screen" on the keyboard while the impersonating profile is displayed. Open Microsoft Paint and navigate to Edit, then Paste. Save the screenshot on your desktop
2. Visit: <https://www.docuSign.net/MEMBER/PowerFormSigning.aspx?PowerFormId=45b4faf1-02e4-4dc2-986f-63152150e6c2> .
3. Enter your name and e-mail address

4. Check your e-mail and use the verification code to confirm your identity
 5. Click on "Review Form" and completely fill-in all fields with as much detail as possible
 6. Place a checkmark in the box next to "Additional Documentation?"
 7. Click attach and upload the screenshot of the impersonating profile
 8. Click "Sign" to complete the form. It will automatically be submitted to LinkedIn
 9. Allow 5 business days for LinkedIn to delete the profile or reply to your e-mail
 10. If you receive no response or the profile is not deleted after 5 business days, e-mail abuse@linkedin.com with information about the impersonating account. Include the full name of the profile and link to it. Explain who you are and attach the screenshot as evidence
 11. For additional details, visit: http://help.linkedin.com/app/answers/detail/a_id/30200/ft/eng
-

(U) MATCH.COM

1. Visit: <http://www.match.com/help/contactus.aspx?ct=1>
 2. Fill out the form completely
 3. Allow 5 business days for Match.com to delete the profile or reply to your e-mail
-

(U) MYSPACE

1. Take a "screenshot" of the impersonating account. To complete this, press "Print Screen" on the keyboard while the impersonating profile is displayed. Open Microsoft Paint and navigate to Edit, then Paste. Save the screenshot on your desktop
 2. Send an e-mail to: compliance@support.myspace.com ONLY FROM AN OFFICIAL GOVERNMENT E-MAIL ADDRESS that includes detailed information about the impersonation and the screenshot
-

(U) SKYPE

1. E-mail abuse@skype.net with information about the impersonating account. Include the full username of the profile and any additional or amplifying details
 2. Allow 5 business days for Skype to reply to your e-mail or delete the account
-

(U) TWITTER

1. Visit: <http://support.twitter.com/forms/impersonation>
 2. Select "I Am Being Impersonated"
 3. Select whether or not you are a representative of the person being impersonated
 4. Complete the contact information
 5. Allow 5 business days for Twitter to delete the account or reply to your e-mail
-

(U) YAHOO

1. Visit: https://io.help.yahoo.com/contact/index?page=contact&locale=en_US&y=PROD_ACCT
2. Select "Abuse and spam" under Topic, "Suspicious email faked from my account" under Sub-topic, and click the "Email" link under "Recommended options"
3. Complete the form on the next page. Under "Yahoo ID", enter your e-mail address
4. After completing the form, click "Create request"
5. Allow 5 business days for LinkedIn to delete the profile or reply to your e-mail
6. Follow the steps outlined in Yahoo's response, including copying/pasting e-mail headers as necessary (Yahoo will include instructions in their response)
7. If no reply is received, e-mail Yahoo at: cc-mailabuse@yahoo-inc.com and provide details of the impersonation

**(U) APPENDIX 2
(U) Law Enforcement Contact Information for Popular Websites**

NOTE: The information contained below is for **LAW ENFORCEMENT USE ONLY**
NOT FOR WIDE DISTRIBUTION

(U) For the most current contact information, and for service provider listings not referenced with in this appendix, please visit: <http://search.org/programs/hightech/isp/> and select the website or service provider from the drop-down menu.

(U) FACEBOOK

(U) As of 2013, Facebook no longer will process law enforcement requests via e-mail or fax. **ALL** requests must be submitted through the Facebook Records website located here: www.facebook.com/records

Contact Address:

Facebook Security, Law Enforcement Response Team
1601 Willow Road
Menlo Park, CA 94025

E-mail Address: records@fb.com

(U) For emergencies or time-sensitive requests, indicate “EMERGENCY REQUEST” in your records request

(U) MICROSOFT SERVICES (HOTMAIL, LIVE.COM, BING.COM, MSN.COM, OUTLOOK.COM, SKYDRIVE)

Contact Address:

Attn: Online Services Custodian of Records
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Phone Number: Switchboard: 425-722-1299

Fax Number: 425-708-0096

(U) Microsoft also has a Digital Crimes Community Portal accessible to law enforcement personnel. Contact dccphelp@microsoft.com to enquire about access

(U) LINKEDIN

(U) LinkedIn has a policy promising to inform users about law enforcement requests. Please follow these recommendations:

- **(U) Preservation notices:** Be aware that your notice to preserve may be disclosed to the target and that you likely cannot get an order to preclude its disclosure
- **(U) Subpoenas and search warrants:** Obtain a 18 USC § 2705(b) notice preclusion order and serve it with your process

(U) Additional details on LinkedIn Law Enforcement Guidelines can be found at the following link: <http://help.linkedin.com/ci/fattach/get/2730181/0/filename/LinkedIn%20Law%20Enforcement%20Guidelines.pdf>

Contact Address:

2029 Stierlin Court, Suite 200
Mountain View, CA 94043

Phone Number: 650-687-3600

Emergency Contact (Business Hours Only): 650-426-6137

Legal Department Fax for Subpoenas: 650-810-2897

(U) MATCH.COM, CHEMISTRY.COM, TINDER

Contact Address:

8300 Douglas Ave, Suite 800
Dallas, TX 75225

Phone Number: 214-576-3236 or 214-576-9341

Fax Number: 214-594-9020 or 214-594-7418

E-mail Address: laurie.latshaw@match.com or norma.rivera@match.com

(U) MYSPACE

(U) The latest MySpace guide for law enforcement personnel can be found using the following link: <https://www.askmyspace.com/t5/Legal-Policy/Law-Enforcement-Guidelines/ba-p/38505>

Contact Address:

Legal Compliance Department
407 N. Maple Drive
Beverly Hills, California 90210

Fax Number: 310-362-8854

E-mail Address: compliance@support.myspace.com

(U) MySpace no longer operates a 24/7 law enforcement support phone line. Please provide a phone number when contacting MySpace via e-mail or fax for their representative to contact you

(U) SKYPE

(U) Although Skype was bought by Microsoft, law enforcement issues are still handled out of Luxembourg

Contact Address:

Skype Communications Sarl

23-29 Rives de Clausen

L-2165

Luxembourg

Phone Number: +011-352-26-19-09-20 (Foreign office, often operator will speak limited English)

Emergency Phone Number (only for life safety issues): +011-352-62-12-73-296

Fax Number: +011-352-26-20-15-82

E-mail Address: LERM@skype.net.

(U) TWITTER

(U) Twitter has a policy promising to inform users about law enforcement requests. Please follow these recommendations:

- **(U) Preservation notices:** Be aware that your notice to preserve may be disclosed to the target and that you likely cannot get an order to preclude its disclosure
- **(U) Subpoenas and search warrants:** Obtain a 18 USC § 2705(b) notice preclusion order and serve it with your process

(U) The best way to contact Twitter for law enforcement matters is through their web form using the following link: <https://support.twitter.com/forms/lawenforcement>

Contact Address:

c/o Trust and Safety - Legal Policy

Twitter Inc.

1355 Market Street, Suite 900

San Francisco, CA 94103

Fax Number: 415-222-9958

E-mail Address: lawenforcement@twitter.com

(U) Refer to Twitter's guidelines for law enforcement personnel on the following website for more information: <http://support.twitter.com/articles/41949-guidelines-for-law-enforcement>

(U) YAHOO (FLICKR.COM, ROCKETMAIL.COM, YAHOO MESSENGER)

(U) For impersonating e-mail accounts that violate Yahoo's Terms of Service (TOS), e-mail cc-mailabuse@yahoo-inc.com with the request. No information about the account will be disclosed to law enforcement.

(U) Yahoo has a policy of explicitly notifying users about government requests for their information prior to disclosure, except when prohibited by law. This does not apply to preservation requests.

(U) When serving Yahoo with legal process, please provide one of the following if you do not want the user to receive notice and time to object:

- (U) A non-disclosure order or citation to applicable law prohibiting disclosure, or
- (U) Facts and circumstances (e.g., imminent threat to life or sexual exploitation of children) sufficient for us to elect, at our sole discretion, to not provide notice.

Contact Address:

Custodian of Records

Yahoo! Inc.

701 First Ave

Sunnyvale, California 94089

Phone Number: 408-349-3687

Fax Number: 408-349-7941

E-mail: lawenforcement-request-delivery@yahoo-inc.com

After-Hours Emergencies: 408-349-5400

(U) To inquire about the status of a request, e-mail: compliance-inquiries@yahoo-inc.com

(U) Additional information on Yahoo guidelines for law enforcement personnel can be found at the following link: <https://transparency.yahoo.com/law-enforcement-guidelines/us/index.html>