Department of Defense

COUNTERINTELLIGENCE FIELD ACTIVITY
WEST

CIFA

SPECIAL REPORT

Production and Use of Fraudulent Military Identification Cards (U)

29 July 2005

(U) Prepared by: CIFA West
CI Analysis Division
Force Protection Branch

(U) Point of Contact: Chris Carver, Chief, Analysis Division
(719) 227-5823, Chris.Carver@cifa.smil.mil

(U) Principal Author: William Martin, CI Analyst, william.martin@cifa.smil.mil

(U) Information Cutoff Date: 27 Jul 05

(U) Executive Summary

(U//FOUO) Primarily, the production and use of fraudulent military identification (ID) cards allows cardholders unauthorized access to DoD facilities and privileges. However, genuine-looking ID cards could be exploited by terrorists to gain entry onto DoD installations. The availability of high-quality printing and reprographic equipment, along with a thriving counterfeit document market on the Internet, makes this a potential threat to force protection. CIFA West assesses that the production and use of fraudulent military ID cards is a small, but significant, portion of a widespread proliferation of counterfeit identification documents.

(U) Recent Reporting

(U//FOUO) During the period 1 Jan 05 - 27 Jul 05, a total of 26 suspicious incidents involving the production and use of fraudulent military ID cards were reported in the Cornerstone and AFOSI databases. Of these reports, three revealed the use of computers and/or stolen forms with the intent to produce fraudulent military ID cards. Seven of the reports described the use of fraudulent military documents. The remaining 16 reports dealt with the use of fraudulent drivers' licenses, immigration ID cards, Social Security cards, and other miscellaneous ID cards.

(U) The following incidents involve the use of computers and/or stolen forms with the intent to produce fraudulent military ID cards:

- (U//FOUO) On 26 Jul 05, three individuals were observed in a restaurant in Yukon, OK, using a laptop computer to produce what appeared to be military ID cards (DD Form 2, US Uniformed Services Retiree ID Card and possibly Common Access Cards). The three individuals were also attempting to use a computer program to change the date of birth on other forms of identification as well (NFI). AFOSI considers this matter closed/unresolved.[1]

- (U//FOUO) On 15 Jun 05, two US Persons (USPERs) were stopped for a traffic violation near Selfridge Air National Guard Base, MI. During the course of the subsequent investigation, multiple items used for counterfeiting military ID cards were seized. The items included 14 sheets of Kodak inkjet photo paper imprinted with the front and back of a DD Form 1173, (Uniformed Service Identification and Privilege Card), four laptop computers, one laminating machine, multiple laminating pouches, one Polaroid camera, and photographs of one of the individuals. FBI and local law enforcement officials continue to investigate.[2]

- (U//FOUO) In Mar 05, a USPER was arrested in KS for passing forged/counterfeit traveler's checks. The USPER was in possession of fraudulent military ID cards, blank ID forms, as well as various cards with his photo with different personal information. IDs with other individuals' names and photos were also saved on his computer. The USPER apparently used his laptop computer and portable printer to produce fraudulent military ID cards and traveler's checks. Individuals in NM (NFI) may also have been involved in this incident. AFOSI considers this matter closed/unresolved. [3]

(U) Historical Perspective

(U) In the last several years, the increased use of the Internet, combined with the advances in computer technology and low production costs, have led to a dramatic increase in the quality and quantity of fraudulent ID cards. Computer technology has made it relatively simple to create the basic template which enables the counterfeit document to be produced. The template can easily be transferred to counterfeiters via email and the Internet. Counterfeiters use the template and sophisticated printing equipment to produce high-quality fraudulent IDs which are then available for purchase.[4]

(U) Until recently, the original method for producing fraudulent ID cards consisted of using a camera, "prefabricated" forms, and a laminator. The person's picture would be cut to fit the size of the paper card and then laminated. This procedure, referred to as the "film base method," required a low initial investment, but the amount of time and labor needed to create a card, or alter its design, dramatically increased the cost per card.[5]

(U) Digital printing revolutionized ID card production by providing fast output and low cost per card. This technology made it easier for counterfeiters to print directly to blank cards and provides unlimited card design and color options. It also enabled counterfeiters to produce genuine-looking security items such as automatic magnetic strips, bar codes, holograms and other smart card options. The latest ID system is comprised of three basic components: a digital camera, computer ID creation software, and an ID card printer.[6]

(U) While individuals can easily obtain fraudulent forms of identification, it is becoming increasingly difficult to distinguish valid forms of ID from counterfeits. The Internet allows the creation and widespread distribution of counterfeit identification that duplicates many of the features of legitimate identification. Special security measures such as holograms, microprinting, and bar codes are already being duplicated by counterfeiters. Despite an increase in actions to stop the manufacture and use of false IDs, the problem continues to grow. Even experienced law enforcement officers may have difficulty detecting false identification.[7]

(U) Common Access Card (CAC) Technology

(U//FOUO) In Nov 99, the DoD initiated procedures to replace the traditional Uniformed Services Identification Card with the Common Access Card (CAC). The CAC was developed to improve information assurance and reduce fraud. The new ID employs "smart card" technology by embedding a computer chip capable of storing the user's personal data in each card. The CAC serves multiple purposes to include functioning as a generic ID card, enabling physical access to DoD buildings, military bases, and other controlled spaces, and granting access to numerous DoD computer networks. Information printed on the CAC includes full name, person designator code (i.e., active duty vs. civilian), rank, Social Security Number, Geneva Convention Category, date of birth, organ donor information, and blood type. Furthermore, other unique information is embedded within the chip such as Public Key Infrastructure (PKI) certificates (ID, e-mail, and encryption), and private authentication materials. [8]

(U//FOUO) The data on the chip is protected by a six to eight digit personal identification number (PIN) created by the user. Although the CAC utilizes state-of-the-art security and authentication methods, security personnel at most military bases and DoD facilities only perform visual inspections of the cards. The mere possession of a stolen card could, in fact, pose a security risk.[9]

(U//FOUO) A limited number of DoD installations have tested a "smart gate" system. This system is designed to improve force protection using advanced technology that verifies authorized personnel to determine if access to the installation should be granted. When an individual drives up to the gate, a CAC or proximity badge is presented to security personnel who place the card into a "reader." The "reader" is a hand-held computer, which allows security and law enforcement personnel to verify a CAC's authenticity through access to the information embedded on the card's computer chip. The personnel identification information is electronically sent to a database where it is cross-referenced to determine if the individual is authorized entry onto the installation.[10]

(U//FOUO) The "smart gate" system is designed to more effectively expedite the flow of authorized individuals onto an installation while allowing security personnel to focus their efforts on unknown individuals and vehicles seeking access to an installation. However, in a recent assessment by the Defense Threat Reduction Agency (DTRA) and the National Security Agency (NSA), key security and exploitation concerns with the middleware and software in the CAC have been revealed, some which have yet to be mitigated.[11] These vulnerabilities could also impact the "smart gate" system.

(U//FOUO) As DTRA and NSA continue to assess the CAC program's vulnerability and security, it is becoming increasingly apparent that no single procedure can guarantee its security or render it impervious to exploitation. The best and most feasible approach to CAC security will likely be the use of multiple technologies, techniques, and procedures within an overall "defense-in-depth" concept. The concept attempts to reduce the various threats while at the same time, striking a balance between security and practicality.[12]

(U//FOUO) Currently, there are no known efforts by foreign entities or adversaries to obtain CAC technology. The Defense Criminal Investigative Service (DCIS) indicates there are ongoing investigative actions involving DoD persons who may be illegally attempting to acquire and black market CAC materials.[13]

(U) Conclusion

(U//FOUO) The production and use of fraudulent military ID cards is a potential significant threat to force protection. The availability of high-quality printing and reprographic equipment, along with a thriving counterfeit document culture, poses a continuing problem for law enforcement personnel attempting to distinquish between fraudulent and genuine forms of identification. Fraudulent but genuine-looking ID cards could be exploited by terrorist groups to gain entry onto DoD installations. CIFA West will continue to monitor developments on this matter.

To comment on this product, please use our feedback link:

http://www.cifa.smil.mil/cifa_west/feedback.html

Endnotes

[1] (U) Air Force Office of Special Investigations (AFOSI) Talon 114-25-07-05-5554

[2] (U) AFOSI Talon 101-29-06-05-5154

[3] (U) AFOSI Talon 321-02-03-05-3749

[4] (U) Testimony to US Senate Committee on Government Affairs, Special Agent David Myers, Fraudulent Identification Unit, Florida Department of Business and Regulations.

[5] (U) Multiple Open Sources

[6] Ibid.

[7] (U) Testimony to US Senate Committee on Government Affairs, Special Agent David Myers, Fraudulent Identification Unit, Florida Department of Business and Regulations.

[8] (U) Criminal Intelligence Bulletin (Intel Bulletin #2004-004), DoD's Common Access Card (CAC), Defense Criminal Investigative Service, 9 Aug 04.

[9] Ibid.

[10] (U) "Force Protection Looking For Volunteers to Test Smart Gate," *The Hansconian*, 4 Oct 02.

[11] (U) Counterintelligence Assessment, DoD Common Access Card (CAC), Critical Infrastructure Protection Division, Counterintelligence Field Activity, 23 Mar 05.

[12] Ibid.

[13] Ibid.