DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON DC 20310-1001

REPLY TO
ATTENTION OF

DAMI-CDS (380)

1 March 2004

MEMORANDUM FOR SEE DISTRUBITION

SUBJECT: Updated Guidance for Installation of Integrated Commercial Intrusion Detection Systems (ICIDS) in Army Sensitive Compartmented Information Facilities (SCIFs)

1. References.

a. Director of Central Intelligence Directive (DCID) 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities, 18 Nov 02.

b. Defense Intelligence Agency (DIA) message, DTG 231549Z Dec 03, Subject: Updated Guidance for Integrated Commercial Intrusion Detection Systems (ICIDS) (Enclosure 1).

c. DIA message, DTG 191319Z Nov 03, Subject: ICIDS (Integrated Commercial Intrusion Detection Systems) (Enclosure 2).

2. A recent DIA review of the Army ICIDS I, II, IIA, and III alarm systems revealed that the ICIDS alarm system contains features/capabilities that do not meet current DCID 6/9 standards. As a result of the review, DIA provided several options that Army Senior Intelligence Officers (SIOs) may implement to bring the SCIF ICIDS alarm system into full DCID 6/9 compliance (references 1a and 1b).

3. While SIOs may choose any of the recommended DIA solutions for their specific ICIDS version installed, some of the DIA recommended solutions are more cost prohibitive and manpower intensive than others. For this reason, ODCS, G-2 (DAMI-CDS) recommends the following:

a. ICIDS I - Install a computer internal to each SCIF to control the alarms for the SCIF and provide only alarm status to the monitoring station with NO remote capabilities. This will ensure that the system administrator is SCI-indoctrinated and no remote capabilities exist within the system.

b. ICIDS II and IIA – Remove the keypad internal to the SCIF and replace with a key switch to put the system into access and security mode. This would eliminate the remote capabilities for the SCIF and provide only an alarm status at the monitoring station.

c. ICIDS III – Install a computer internal to each SCIF for control of the SCIF alarms. This will provide only an alarm status to the monitoring station with NO remote capabilities. The alarm system must have 128 bit encryption and a National Institute Certification of Standards and Technology (NIST) certificate. The SIO, Special Security Officer (SSO), and/or the Special Security Representative (SSR) will ensure that the NIST certificate is maintained with the SCIF accreditation documentation.

4. SIOs should continue to work closely with their installation Provost Marshall Office or Law Enforcement Activity to ensure appropriate representation and participation at meetings where installation of alarm systems in Army SCIFs, to include ICIDS, is being proposed. Additionally, SIO/SSO/SSR must ensure you maintain ongoing coordination with DIA prior to any alarm system modification and/or installation.

5. Request Major Command, Direct Reporting Units, and Field Operating Activities SIOs provide the following SCIF information NLT 15 Apr 04 for each subordinate SCIF with an installed ICIDS alarm system. This office will consolidate your input and forward to DIA.

a. SCIF Number and location.

b. ICIDS alarm version, e.g., ICIDS I, II, IIA or III (If not yet installed, provide projected installation date and version).

b. Projected timeline for corrective action to be taken and solution chosen.

c. SCIF SSO/SSR name, phone number, and email address.

6. The POCs for this action are Ms. Autry, DSN 225-2647/CM 703 695-2647 or Ms. Morisse, DSN 225-2645/CM 703 695-2645.

Encl (2)

FOR MICHAEL T. RASCATI
Acting Director, Counterintelligence, HUMINT, Disclosure & Security

DISTRIBUTION:
ADMINISTRATIVE ASSISTANT TO THE SECRETARY OF THE ARMY
(HQDA SSO/DIRECTOR OF SECURITY AND SAFETY)

CHIEF, U.S. ARMY NATIONAL GUARD BUREAU (NGB)
DAMI-CDS (380)
SUBJECT: SUBJECT: Updated Guidance for Integrated Commercial Intrusion Detection Systems (ICIDS)

U.S. ARMY MATERIEL COMMAND (AMCGS)
U.S. ARMY FORCES COMMAND (AFIN)
U.S. ARMY TRAINING AND DOCTRINE COMMAND (ATIN)
UNITED STATES ARMY AND SEVENTH US ARMY EUROPE (AEAGB)
U.S. ARMY MEDICAL COMMAND (MCOP)
U.S. ARMY CORPS OF ENGINEERS (CECS)
EIGHTH U.S. ARMY (EAGB)
U.S. ARMY SPACE MISSILE AND DEFENSE COMMAND (SMDC-ZB)
U.S. ARMY SPECIAL OPERATIONS COMMAND (AOIN)
U.S. ARMY PACIFIC (APIN)
U.S. ARMY SOUTH (SOIN)
U.S. ARMY MILITARY DISTRICT OF WASHINGTON (ANOP-S)
U.S. ARMY CRIMINAL INVESTIGATION COMMAND (CICG)
U.S. ARMY INTELLIGENCE AND SECURITY COMMAND (IASE)
MILITARY TRAFFIC MANAGEMENT COMMAND (MT)
U.S. ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9th ARMY SIGNAL COMMAND
U.S. ARMY OPERATIONAL TEST AND EVALUATION COMMAND (CSTE)

CF:
HQDA SSO (LTC Carroll)
ODCS, G-3 (DAMO-ODL) (Mr. Parsons)
DIA DAC2A (Ms. Truchon)

DTG: 231549Z DEC 03 PAGE 01 of 03

Drafter's Name : P SAGER-DEAN, SPECIAL PROJ
Office/Phone : DAC-2A 0938
Releaser's Info : P. TRUCHON,BR CH,DAC-2,1300

Action Prec : ROUTINE
Info Prec : ROUTINE
Specat :

From: SSO DIA//DAC-2A//
To: SSO USAF//XOII-CSA//
SSO DA//DAMI-CHS//
SSO NAVY//522//
SSO NIMA//RES/BET//
SSO DIA//DAC-2C PENTAGON SATELLITE OFFICE//
ALORS
Info: SAFE

TEXT FOLLOWS

UNCLASSIFIED

QQQQ

SUBJECT: UPDATED GUIDANCE FOR INTEGRATED COMMERCIAL INTRUSION DETECTION SYSTEMS (ICIDS)

REF: SSO DIA/DAC-2A MSG DTG 191319Z NOV 03

1. THE FOLLOWING IS PROVIDED FOR CLARIFICATION OF THE GRANDFATHER CLAUSE IN REFERENCE. FOR THOSE FACILITIES THAT HAVE ICIDS 1, 2, OR 2A INSTALLED AND CURRENTLY ACCREDITED, THE ALARM SYSTEM MUST BE CONFIGURED AS STATED IN ABOVE REF. IF THESE SYSTEMS ARE NOT CONFIGURED AS STATED, THE ALARM SYSTEM IS NOT GRANDFATHERED AND MUST COMPLY WITH REGULATIONS FOR SCIFS.

2. AS DISCUSSED WITH THE ALARM CONTRACTORS FOR THE VARIOUS VERSIONS OF ICIDS, THE FOLLOWING IS PROVIDED TO ASSIST THE MAJOR COMMANDS, BASES AND POSTS TO BRING ICIDS INTO COMPLIANCE BY ONE OF THE FOLLOWING OPTIONS:

A. ICIDS 1 OPTIONS:

OPTION 1: THE SYSTEM MUST BE PASSWORD PROTECTED AT THE CENTRAL MONITORING STATION AND THE SYSTEM ADMINISTRATOR MUST BE SCI-INDOCTRINATED DUE TO THE REMOTE CAPABILITIES OF THE SYSTEM. SCIF MANAGERS MUST CONDUCT RANDOM CHECKS OF THE HISTORICAL RECORDS OF ALL EVENTS. MAINTAIN ON FILE RECORDS OF ANY ALARM ANNUNCIATIONS FOR A MINIMUM OF 90 DAYS OR UNTIL INVESTIGATION OR SYSTEMS VIOLATIONS AND INCIDENTS HAVE BEEN SUCCESSFULLY RESOLVED AND RECORDED. ADDITIONAL COSTS WILL BE INCURRED DUE TO CLEARING OF PERSONNEL.

ENCL 1

OPTION 2: DESIGNATE A SINGLE SCI ADMINISTRATOR OF THE ALARMS FOR SCIFS ON BASE. ADDITIONAL COSTS WILL BE INCURRED DUE TO ADDITIONAL CABLES, A COMPUTER TO ADMINISTER THE ALARMS, AND MODEMS TO COMMUNICATION TO THE ADMINISTRATION COMPUTER. PERSONNEL IN THE SCIFS WOULD OBTAIN THEIR PINS AND ACCESS CODES AT THE ALARM ADMINISTRATIVE SCIF. SCIF MANAGERS MUST CONDUCT RANDOM CHECKS OF THE HISTORICAL RECORDS OF ALL EVENTS. MAINTAIN ON FILE RECORDS OF ANY ALARM ANNUNCIATIONS FOR A MINIMUM OF 90 DAYS OR UNTIL INVESTIGATION OR SYSTEMS VIOLATIONS AND INCIDENTS HAVE BEEN SUCCESSFULLY RESOLVED AND RECORDED.

OPTION 3: THE BEST SOLUTION FOR THE SYSTEM IS TO INSTALL A COMPUTER INTERNAL TO EACH SCIF TO CONTROL THE ALARMS FOR THE SCIF AND PROVIDE ONLY ALARM STATUS TO THE MONITORING STATION WITH NO REMOTE CABILITIES. THIS WOULD ENSURE THAT THE SYSTEM ADMINISTRATOR IS SCI-INDOCTRINATED AND NO REMOTE CAPABILITIES EXIST IN THE SYSTEM. ADDITIONAL COSTS WOULD BE INCURRED.

B. ICIDS 2 AND 2A OPTIONS:

OPTION 1: FOR THOSE SYSTEMS MONITORED AT A CENTRAL MONITORING STATION OR CENTRALLY LOCATED IN ANOTHER SCIF, THE REMOTE CAPABILITIES TO SHUNT OR MASK ALARMS MUST BE REMOVED. (REMOVAL OF THE REMOTE CAPABILITIES WOULD NOT ALLOW THE SYSTEM TO PARTITION SCIFS FROM NON-SCIF AREAS; WOULD REMOVE ALL REMOTE CAPABILITIES FOR ALL NON-SCIF AREAS AS WELL AS SCIF'D AREAS AND REQUIRE THAT ALL FACILITIES FOR THE COMMAND, BASE OR POST BE ADMINISTERED BY AN SCI-INDOCTRINATED PERSON TO MEET DCID 1/21, ANNEX B STANDARDS.) THE SYTEM ADINISTRATOR MUST BE SCI-INDOCTRINATED. SCIF MANAGERS MUST CONDUCT RANDOM CHECKS OF THE HISTORICAL RECORDS OF ALL EVENTS. MAINTAIN ON FILE RECORDS OF ANY ALARM ANNUNCIATIONS FOR A MINIMUM OF 90 DAYS OR UNTIL INVESTIGATION OR SYSTEMS VIOLATIONS AND INCIDENTS HAVE BEEN SUCCESSFULLY RESOLVED AND RECORDED. ADDITIONAL COSTS WILL BE INCURRED DUE TO CLEARING OF PERSONNEL.

OPTION 2: THE BEST SOLUTION FOR THIS SYSTEM IS TO REMOVE THE KEYPAD INTERNAL TO THE SCIF AND REPLACE WITH A KEY SWITCH TO PUT THE THE SYSTEM INTO ACCESS AND SECURE MODE. THIS WOULD ELIMINATE THE REMOTE CAPABILITIES FOR THE SCIF AND MONITORING WOULD OCCUR ONLY AT THE MONITORING STATION. THIS WOULD INCUR ADDITIONAL COST FOR THE MODIFICATION.

C. ICIDS 3 OPTIONS:

OPTION 1: THE BEST SOLUTION FOR THIS SYSTEM IS TO INSTALL A COMPUTER (PCU) INTERNAL TO EACH SCIF FOR CONTROL OF THE ALARMS. THIS WOULD PROVIDE ONLY AN ALARM STATUS TO THE MONITORING STATION WITH NO REMOTE CAPABILITIES. THE SYSTEM MUST HAVE 128-BIT ENCRYPTION AND A NIST CERTIFICATE MUST BE MAINTAINED ON FILE.

OPTION 2: FOR THOSE SYSTEMS CONTROLLED AT THE CENTRAL

MONITORING STATION, THE SYSTEM MUST BE PARTITIONED SEPARATING SCIF FROM NON-SCIF FACILITIES. THE SYSTEM ADMINISTRATOR MUST BE SCI-INDOCTRINATED AND THE SYSTEM PASSWORD PROTECTED. THE SYSTEM ADMINISTRATOR WILL CONDUCT RANDOM CHECKS OF THE HISTORICAL RECORDS OF ALL EVENTS. FILE RECORDS WILL BE MAINTAINED FOR A MINIMUM OF 90 DAYS OR UNTIL INVESTIGATIONS OF SYSTEM VIOLATIONS AND INCIDENTS HAVE BEEN SUCCESSFULLY RESOLVED AND RECORDED. THE NETWORK ADMINISTRATOR MUST BE TOP SECRET CLEARED. THE SYSTEM MUST HAVE 128 BIT ENCRPTION AS INDICATED ON THE NIST CERTIFICATE MAINTAINED WITHIN THE FACILITY. DUE TO THE RMS BEING AT THE CENTRAL MONITORING, THE CENTRAL MONITORING STATION WOULD HAVE TO BE A SCIF.

OPTION 3: FOR THOSE SYSTEMS THAT THE MAJOR COMMAND, BASE OR POST HAS DESIGNATED ONE SCIF TO ADMINISTER THE ALARMS FOR SCI FACILITIES. ADDITIONAL INFRASTRUCTURE WOULD BE REQUIRED TO ACCOMMODATE THIS OPTION, SUCH AS ADDITIONAL MODEMS, LINES BETWEEN FACILITY AND EXTERNAL FACILITIES, RMS WORKSTATION AT CENTRAL SCIF, ENCRYPTION DEVICES, AND MUX BOARDS. THE SYSTEM ADMINISTRATOR WILL CONDUCT RANDOM CHECKS OF THE HISTORICAL RECORDS OF ALL EVENTS. FILE RECORDS WILL BE MAINTAINED FOR A MINIMUM OF 90 DAYS OR UNTIL INVESTIGATIONS OF SYSTEM VIOLATIONS AND INCIDENTS HAVE BEEN SUCCESSFULLY RESOLVED AND RECORDED. THE SYSTEM MUST HAVE 128 BIT ENCRPTION AS INDICATED ON THE NIST CERTIFICATE MAINTAINED WITHIN THE FACILITY. THE ONE MAIN PROBLEM WITH THIS OPTION IS IF THE ORGANIZATION THAT CONTROLS THE FACILITY THAT HOUSES THE COMPUTER TO ADMINISTER THE ALARMS COULD GO AWAY OR NOT HAVE A REQUIRE FOR AN SCI MISSION AND WOULD CAUSE THIS TO HAVE TO BE MOVED TO ANOTHER SCIF.

3. PROVIDE A STATUS OF CORRECTIONS TO DIA/DAC-2A FOR THOSE POST/BASES THAT ARE CONFIGURED AS STATED ABOVE BY 31 JANUARY 2004. FAILURE TO TAKE ACTION TO RESOLSE THIS ISSUE MAY JEOPARDIZE THE ACCREDITATION OF ALL FACILITIES ON A BASE POST BUILDING, OR COMPOUND IF FOUND DURING AN INSPECTION.

4. PROJECT OFFICER FOR THIS ACTION IS PAT SAGER-DEAN AT:
COMM: (703) 907-0938
DSN: 283-0938

5. QUESTIONS OR CONCERNS CAN BE DIRECTED TO THE ABOVE OR TO DIA/DAC-2A AT:
COMM: (703) 907-1299
DSN: 283-1299
JWICS EMAIL: DIEM120@DIA.IC.GOV (ALL LOWERCASE)
SIPNET EMAIL: DICM102@NOTES.DAWN.DIA.SMIL.MIL (ALL LOWERCASE)

DTG: 191319Z NOV 03 PAGE 01 of 02

Drafter's Name : P SAGER-DEAN, SPECIAL PROJ
Office/Phone : DAC-2A, 0938

Releaser's Info : P. TRUCHON, BR CH, DAC-2, 1300

Action Prec : ROUTINE
Info Prec : ROUTINE
Specat :

From: SSO DIA//DAC-2A//
To: SSO DA//DAMI-CHS//
SSO USAF//XOII-CSA//
SSO NAVY//522//
ALORS
SSO NIMA RES
SSO DIA//DAC-3C PENTAGON SATELLITE OFFICE//
SSO DTRA ALEX
Info: SAFE

TEXT FOLLOWS

UNCLASSIFIED

QQQQ
SUBJECT: ICIDS (INTEGRATED COMMERICAL INTRUSION DETECTION SYSTEMS)
1. DAC-2A HAS CONDUCTED A THOROUGH REVIEW OF ICIDS AND THE FOLLOWING INFORMATION IS PROVIDED:
A. ICIDS I (PROVIDED BY LOCKHEED MARTIN): THIS SYSTEM WAS APPROVED IN THE LATE 1980'S AND HENCE IS GRANDFATHERED. THEREFORE, ALL FACILITIES THAT HAVE THIS EQUIPMENT INSTALLED WITHIN THEIR FACILITY MUST ENSURE THE SYSTEM IS PASSWORD PROTECTED AT THE CENTRAL MONITORING STATION AND THE SYSTEM ADMINISTRATOR FOR THE SYSTEM IS SCI-INDOCTRINATED. THIS IS DUE TO THE REMOTE CAPABILITIES OF THE SYSTEM. SCIF MANAGERS MUST ALSO CONDUCT RANDOM CHECKS OF THE HISTORICAL RECORDS OF ALL EVENTS, EITHER AUTOMATICALLY OR THROUGH THE USE OF A MANUAL LOG SYSTEM FOR THE FACILITY. RECORDS OF ALARM ANNUNCIATIONS SHALL BE RETAINED FOR AT LEAST 90 DAYS OR UNTIL INVESTIGATIONS OF SYSTEM VIOLATIONS AND INCIDENTS HAVE BEEN SUCCESSFULLY RESOLVED AND RECORDED. (DCID 1/21, ANNEX B, PARA 3.8.7)
B. ICIDS II AND IIA (PROVIDED BY LOCKHEED MARTIN): THIS WAS A MODIFICATION TO ICIDS I AND APPROVED PRIOR TO 18 NOVEMBER 2002 AND THEREFORE, GRANDFATHERED UNDER DCID 1/21. LOCKHEED MARTIN HAS AGREED TO REMOVE ALL REMOTE CAPABILITIES AND PARTITION THE SCIFS FROM THE MONITORING STATION PERMITTING MONITORING PERSONNEL TO MONITOR ONLY. THE REMAINING ISSUE OF PROVIDING PIC (PERSONAL IDENTIFICATION CODE) OR PIN (PERSONAL IDENTIFICATION NUMBER) FOR ACCESSING AND SECURING THE ALARMS WILL MEAN THAT ONE OF THE FOLLOWING OPTIONS IS ACCEPTABLE:
(1) THE IDS SYSTEM ADMINISTRATOR MUST BE SCI-INDOCTRINATED;
(2) PROVIDE A TERMINAL FOR INPUTTING PIC AND PIN'S INTERNAL TO EACH SCI FACILITY OR INTERNAL TO A SINGLE SCI FACILITY ON THE BASE OR COMPOUND; OR

ENCL 2

(3) PROVIDE A SEPARATE TERMINAL AT THE CENTRAL MONITORING STATION FOR SCIF PERSONNEL OR AN SSO TO ENTER AND ISSUE PIN AND PIC NUMBERS PERMITTING ONLY ASTERISKS TO APPEAR WITHIN THE ACTUAL SYSTEM ITSELF.

C. ICIDS III (PROVIDED BY RADIAN INC): THIS SYSTEM WILL BE CONFIGURED TO HAVE 128-BIT ENCRYPTION FOR LINE SUPERVISION AND NO REMOTE CAPABILITIES FROM THE MONITORING STATION. THIS WILL ALSO REQUIRE THE FOLLOWING:

(1) THE SSO OR EACH SCIF WILL ADMINISTER THEIR IDS PROVIDED BY A REMOTE STATUS MONITOR (RSM) OPERATOR WORK STATION THAT IS INTERNAL TO THE SCIF AND PARTITIONED FROM THE NON SCI FACILITIES. IF THE ACCESS CONTROL SYSTEM IS ALSO TO BE REPLACED, THIS WOULD PERMIT SSO/SCIF SECURITY PERSONNEL ADMINISTER THEIR ACCESS CONTROL SYSTEM ALSO; OR

(2) THE SYSTEMS ADMINISTRATOR MUST BE SCI-INDOCTRINATED AND THE NETWORK INTRUSION DETECTION SYSTEMS ADMINISTRATOR (NIDS) MUST BE CLEARED FOR TOP SECRET, AND THE RSM (PARTITIONED FROM THE NON-SCI FACILITIES) THAT CONTROLS THE SCIF ALARMS MUST BE PLACED INTERNAL TO A SCIF. A NIST AND UL CERTIFICATE ARE REQUIRED FOR CONTRACTORS AND A NIST CERTIFICATE ONLY FOR THE BASES.

2. PROVIDE A STATUS OF CORRECTIONS FOR THOSE BASES/CONTRACTORS THAT ARE NOT CONFIGURED AS STATED ABOVE NLT 31 JANUARY 2004. FAILURE TO PROVIDE THIS INFORMATION MAY JEOPARDIZE THE ACCREDITATION OF ALL FACILITIES ON A BASE, BUILDING, OR COMPOUND IF FOUND DURING AN INSPECTION.

3. DIA/DAC-2A PROJECT OFFICERS ARE MS. PAT SAGER-DEAN OR SFC TERRY TAYLOR, (703) 907-0938/2887 OR DSN 283-0938/2887.