Enabling certification, accreditation across a theater of operations

Enabling certification, accreditation across a theater of operations

By LTC Michael Lanham, Thelma Wandhal-Bundesen, Donald DeLaHunt, Michael Charbonneau

Certification and accreditation of network enclaves allows Army service component commanders and their designated approving authorities to have a formal and repeatable process of identifying, measuring, mitigating and accepting risks to a critical command and control enabler—their communications networks.

The authors, and a team of professionals from the ASCC headquarters, the 335th Signal Command (Theater) (Provisional), and the 160th Signal Brigade, improved the C&A posture of USARCENT. The improvement allows USARCENT to better know what risks the command is formally accepting, as well as identify risks it had been informally accepting but did not truly know about.

There are many official definitions of Information Assurance and C&A. We'll review some of those definitions in the course of this article, but prefer an unofficial definition that is more readily accessible to operational forces and maneuver commanders.

IA is informed risk management and risk acceptance. C&A is a formal and repeatable way to identify, assess, reduce and accept risks for network enclaves. Risk acceptance, especially in environments with high personnel turbulence/turnover, should occur formally. Risk acceptance processes should support continuity of knowledge and understanding of the acceptance rationale.

An analogy between the Military decisionmaking process and C&A is appropriate at this point. MDMP is a formal and structured way to plan missions, including identifying and reducing the risks within those missions. C&A is a formal and structured way to plan the deployment and employment of network enclaves, including identifying and reducing the risks to the maneuver or operational commanders those networks support.

FM 5-0 Army Planning and Orders Production is the doctrinal basis for the Army's use of MDMP. For C&A, the doctrinal basis is in a trail of documents starting at Department of Defense Directive 8510.01 DoD IA C&A Process. The trail continues to the Chairman Joint Chiefs of Staff Instruction 6510.01E IA and Computer Network Defense, to combatant command policies and regulations and for Army units, ends in Army Regulation (AR) 25-2 Information Assurance.

The status quo for most Army network enclaves generally falls into one of three categories: no C&A at all; informal C&A; and formal C&A. Long-term members of Functional Areas 24 and 53 and members of the Signal Regiment will recall, with varying levels of nostalgia, enclaves they have built, sustained, maintained and operated without the faintest evidence of C&A activities. More likely, based on an unscientific sampling of the Army's Portfolio Management System, Army network enclaves and information systems fall into an informal C&A status—DAAs authorize operations of enclaves without being fully DIACAP-compliant and without truly knowing what risks they are accepting on behalf of their commander.

Informal C&A was, and in many cases still is, a reasonable course of action for Commanders and DAAs to use. Informal C&A is considerably less expensive in up-front costs as well as long-term costs, thereby meeting DoDD 8500.01E guidance to, in the Commander's assessment, balance the five pillars of IA, the importance and sensitivity of network enclaves, threats, and costs. However, there are a number of risks associated with the informal nature of the C&A.

Those risks include: the lack of an independent, outside-the-command review of IA controls; potential for not using DoD standard IA controls and assessment methods; and decisions based on deliberately incomplete information. Risks also include: creation of a risk-acceptance culture by persons and units without the command responsibility and authority to accept risks; and inflicted risk when these network enclaves interconnect to the rest of the theater information grid and the Global Information Grid.

The authors developed and recommended to the DAA a staggered implementation plan to resource and execute formal, DIACAP-compliant C&A efforts for all of USARCENT's network enclaves. In this case the DAA simultaneously served as the USARCENT G6 and 335th SC(T)(P) commander. With the DAA's approval, USARCENT began its efforts in September 2008. Efforts continue to the present time expanding the formal C&A

activities maintaining the formal accreditations now in place.

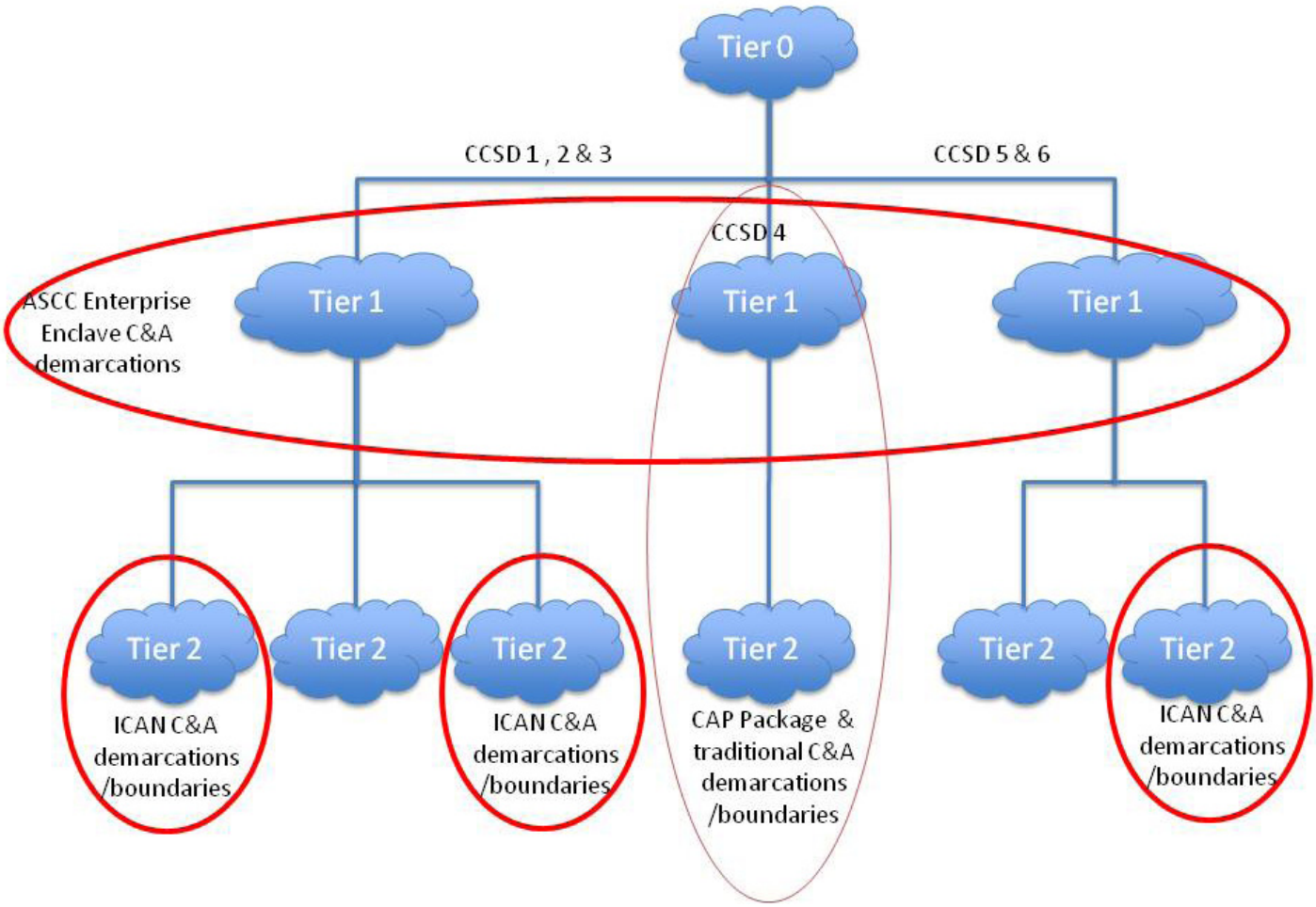
One of the first challenges we faced was defining what network enclaves existed within USARCENT.

In the U.S. Central Command area of responsibility, USARCENT directly commands and controls almost a dozen posts, camps and stations (P/C/S). Each P/C/S has one or more classification domains for their network enclaves (e.g. NIPRNet, SIPRNet, and various flavors of Coalition Enterprise Information Exchange).

We used the existing circuit action process packages for the communications circuits connecting USARCENT to the GIG as the staring point for identifying our enclaves. The team was able to identify all the circuits feeding network capabilities into USARCENT as well as the existing network diagrams for Tier 1 and Tier 2 enclaves. Figure 1 depicts, for operational security reasons, notional circuits between the Defense Information Systems Agency managed Tier 0 network cloud to the USCENTCOM-managed, Southwest Asia Theater Network Operations Center operated Tier 1. Below Tier 1 are the individual P/C/S Tier 2 network enclaves operated by the 54th Signal Battalion and its assigned companies. An important note for readers: USARCENT does not have network enterprise centers or directorates of information management in any of its task organization documents or charts. USARCENT does have a supporting signal trace under a clear joint staff and USCENTCOM directed line of command and control leading back to the ASCC commander.

With permission from the DAA, and the USCENTCOM IA manager, we aligned our accreditation (and future CAP actions as well) boundaries with the Army's Best Business Practice for the C&A of installation campus area networks. We did not align the enclave boundaries from Tier 1 through Tier 2 like CAP packages (the vertical oval in the center of Figure 1 encompassing command communications service designator 4). Instead, we choose to build a hierarchy of network enclaves. That hierarchy would allow lower levels to inherit IA controls from higher levels. We created a logical definition of the USARCENT NIPRNet enterprise enclave that became the top of our C&A hierarchy (the horizontal oval in Figure 1 encompassing all the Tier 1 touch points). The second, and lower tiers of our C&A

(Continued on page 38)



(Continued from page 37)

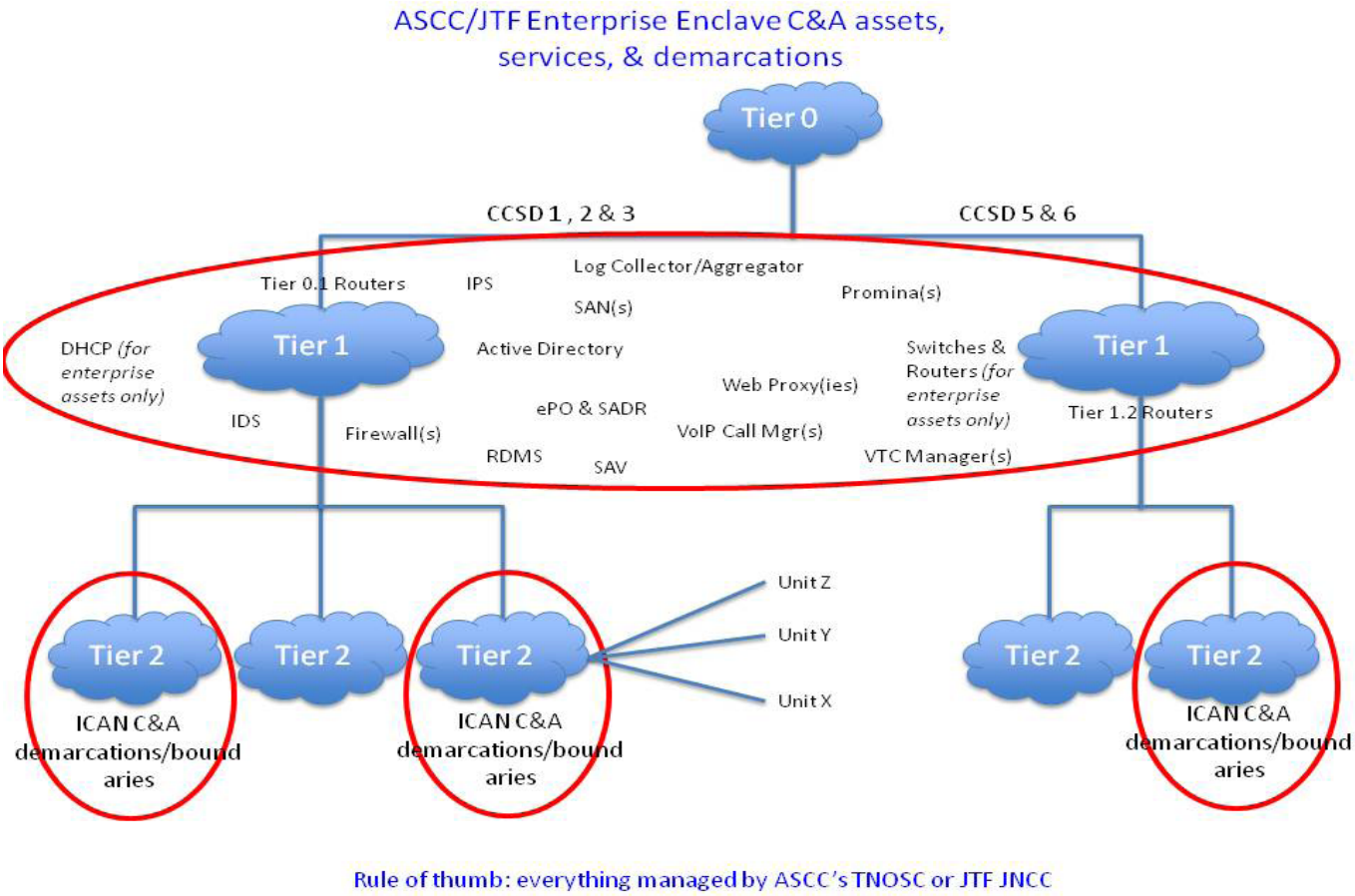
hierarchy included each P/C/S' ICANs. The second tier also includes special purpose enclaves built by individual units or organizations that connected to the P/C/S ICANs.

The logical demarcations for the enterprise enclave were simple in concept. The concept proved, initially, difficult for the USCENTCOM IA staff, Army Certification Authority, the Agent of the Certifying Authority, the supporting Signal units, and the contracted assessment team to grasp. This was the first time they had ever seen this deliberate construction of a C&A hierarchy. The rule of thumb was straightforward. Everything the SWA-TNOSC and Regional Computer Emergency Response Team-SWA directly managed for the benefit of the entire task organization was part of the USARCENT enterprise enclave. Anything below that was an ICAN. Figure 2 shows a representative sample of capabilities and network infrastructure that became the baseline for the USARCENT NIPRNet enterprise enclave.

USCENTCOM IA, the CA and the rest of the C&A community eventually concurred with our approach citing the future benefits. We expect that future C&A efforts for each of the ICANs at the individual P/C/S will have a net reduction in labor and certification costs. ICANs will be able to inherit ASCC-wide IA controls, policies, and capabilities (e.g. network tactics, techniques, and procedures, perimeter protection, host/system protection). Cost reduction should be a key factor in future C&A efforts at USARCENT--due to the forward-deployed locations, visa requirements and other reasons, ACA visits to the USCENTCOM AOR were significantly more expensive than costs and estimates the authors, and others, previously experienced in the Continental United States.

We began the C&A effort by completing an initial ACA scoping questionnaire. The questionnaire allows an ACA to provide an informed estimate of resources they need (e.g. labor, travel, administrative costs). We then established a backward planning timeline to drive the completion of C&A for the NIPRNet and SIPRNet Enterprise Enclaves by July 2009 and January 2010, respectively.

For the 335th SC(T)(P) IAM and G3 then dedicated contractor support to provide the day-to-day execution of the preparations for the visit. The preparations included the following:



completing and finalizing the ACA scoping questionnaire; authoring and modifying the System Identification Profile; and authoring and maintaining a self-assessed DIACAP implementation plan. Preparations also include: authoring and maintaining a self-assessed DIACAP scorecard; authoring and updating the Plan of Actions and Milestones for known and discovered deficiencies; and coordinating interviews with personnel from SWA-TNOSC, RCERT-SWA, and 54th Signal Battalion Regional NOSC. USARCENT conducted the coordination with the ACA for their visit and kept track of progress to brief to senior leadership. USARCENT's Main Command Post in Atlanta also played a key role, even in the midst of its own C&A activities for its HQs ICANs. The MCP registered the Enterprise Enclaves into the APMS. Registration into APMS is critical to gaining access to the Army's CA and formalizing the entire C&A process.

A critical task for the C&A team was involvement of the ASCC Commander. The IAPM and DAA wanted the commander's direct involvement in establishing the Mission Assurance Category for his Enterprise enclaves. Anything less than MAC I entailed deliberate, informed acceptance of risk. Before the commander would do that, we had to provide information briefings and papers to refresh the key leaders' understanding of IA as well as mission assurance. Additionally, we had to explain, with specificity, the regulatory and doctrinal framework and requirements that, we believed, required the commander's personal involvement. The USARCENT commander signed the memorandum for record establishing the MAC level for the enterprise enclave and placed C&A status updates onto the calendar.

Another significant preparatory task was the collection of evidence and artifacts to substantiate the self-assessed score for the IA controls. In effect, the collection allowed the command to rehearse the data collection and interviews the ACA assessment team would execute. The enclave IA controls, over 100 of them, had assessment criteria that Soldiers who have executed ARTEPS and EXEVALS would, minus the technical jargon, instantly recognize. Each IA control is equivalent to an ARTEP task with accompanying conditions and standards. The tasks group were divided into eight categories, allowing the creation of eight books/collections of evidence. It was vital, in the teams' assessment, to prevent the generation of any one-off or just-for-the-assessment artifacts and documents. The team wanted evidence of the as-built, as-executed state of the network enclave, not specially created artifacts that would not be accurate past the day of the assessment.

The final preparatory task under consideration here is the communications plan the C&A team executed. The communications effort was for the ASCC leadership, the supporting Signal commands' leadership and staff. It was also for the Soldiers, DA civilians and contractors that had built, operate and continue enhancing more than 30 USARCENT network enclaves. The communications plan had four goals. The first goal was to defeat the perception that the C&A effort was going to feed negative performance reports and impact contract performance awards. The second goal was to convince the day-to-day enclave operators and maintainers that C&A had to reflect what they actually did to allow the DAA to make informed decisions. The third goal was to convince leadership at all levels that discovered non-compliance with any particular control was a starting point for risk management and reduction. The final goal was to set the stage for the C&A effort to be sustainable and not a one-off bureaucratic paper drill.

The 335th SC(T)(P) contract support to the C&A effort, along with efforts by the SWA-TNOSC, RCERT-SWA, and the authors set the stage for the ACA visit to Kuwait in March 2009. The team of contractors conducted an in brief with the DAA, the USARCENT Deputy G6, the IAPM, the 335th SC(T)(P) G3, and the 160th Signal Brigade Commander. The USARCENT and 160th Signal Brigade IA staff then conducted an orientation briefing to the team. The ACA team had never, as noted above, experienced as complex of an environment as USARCENT faced. The weekly pre-arrival coordination teleconferences had not adequately conveyed the scope of the effort—a significant concern given USARCENT had more than 30 additional enclaves to accredit. The team adapted, and began their interviews, technical data collection and walk-through of facilities. The team also took possession of the artifact collections built before their arrival.

Interviews with technicians, Soldiers, and supervisory chains became the most interesting and challenging component of the assessment. The interviewees took to heart the authors' guidance to hold nothing back, hide nothing, and let the DAA know of every risk. The ACA team and the command discovered new areas of non-compliance and risks previously unknown. The DAA and IA program manager had expected discovery learning, what we had not anticipated

(Continued on page 40)

(Continued from page 39)

was the absence of interviewees that had gone through the preparations for the actual ACA visit. Those absences allowed an opportunity for the entire C&A team to discover that information flow and knowledge distribution within the visit participants was not optimal. We took that lesson and applied it to the subsequent ACA visit in December 2009 for the SIPRNet Enterprise Enclave. The out-brief was a testament to the dedication and professionalism of USARCENT's supporting signal units—there were no Category 1/Critical findings, a small number of Category 2 findings and the Category 3 findings were generally known due to the preparation prior to the ACA visit.

The post-assessment visit phase of the C&A was when the C&A team began the construction of the Plan of Actions and Milestones. The POA&M for a C&A package is the formal means by which the DAA tracks the status of risk reduction efforts. It's also the tool by which the DAA formally accepts by-item residual risks. The ACA team collaborated on the POA&M development, as a finalized and signed POA&M is a necessary part of their recommendation package to the Army CA. The CA, because of the Category 2 findings, recommended a six-month Interim-Authority to Operate. Using the authorities CJCSI 6510.01E enumerates, and with USCENTCOM concurrence, USARCENT's DAA issued a three-year Authority to Operate. He also imposed a fast corrective POA&M for the Category 2 findings. This ATO was then a key component to achieving the first alignment of expiration dates for all of USARCENT's NIPRNet circuits with USCENTCOM. That alignment greatly reduces the labor costs associated with recurring non-aligned CAP package submissions.

USARCENT has registered in APMS two of its Enterprise Enclaves and attained DIACAP-compliant ATOs for both. It, and its supporting signal units, must now transition to sustainment of those ATOs. USARCENT must also continue providing resources to its supporting signal commands to enable them to succeed at gaining DIACAP-compliant accreditations of the ICANs at each P/C/S. It remains to be seen whether USARCENT, in coordination with Army's CA, will develop its own ACA capability to dramatically reduce costs. Future rotations of USARCENT staff, IAPMs, IAMs, along with the supporting signal commands will assume the responsibility of helping the USARCENT Commander and DAA conduct informed risk management and risk acceptance for his network enclaves.

For Army leaders to stimulate across the board improvement in adherence to policy and regulatory requirements, commanders and their DAAs will need help. There are few Soldiers as well positioned to provide that help as the officers in the Signal Regiment Functional Areas 24 and 53. We can, and must, change the common perceptions of IA and C&A. Unless you have your head buried in the sand, you most certainly have heard or been stymied by one of the common perceptions articulated that IA and C&A are: a task to avoid; a burden to starve of resources and interest; a paper-drill that is inaccurate the moment it completes; unresponsive to unforeseen requirements; unwilling to accept short-term risks; unable to transition between short-term risks and long-term risk reduction; incapable of communicating to operational force and maneuver commanders why particular (or general) computer network risks deserve their attention compared to the other risks they deal with every day; unable to communicate to specific commanders that it is their device(s) or Soldier(s) causing a problem; and finally, that computer network defense and security is the job of the "Six" so stop bothering the commander or the S3/G3/J3.

Here are some important points we offer to spark discussions on how to help both operational and non-operational commanders make better informed risk decisions for their supporting computer network enclaves.

- Incorporate attaining and maintaining DIACAP-compliant accreditations into theater Signal command and brigade leadership performance reports
- Explore the probability that military and DA civilian ACA teams are less expensive in the long term than contracting out services
- Formal DIACAP compliance in Coalition/Joint Task Force environments may not be possible, but informed risk management by the JTF Commander should still be feasible—weighed against other operational imperatives as the JTF commander assesses.
- Make C&A supporting processes (e.g. change management boards, configuration management boards, IAVA and system patching, requests for new capabilities/services, help desk/trouble ticketing systems) responsive to unforeseen needs. Key to this is changing the seemingly reflexive and automatic 'IA says no' to 'yes, and let's see how we can do it safely given our time and resource constraints.'

• Units should capture risk acceptance decisions in artifacts and documents. Doing so allows a continuity of knowledge and potential reduction in revisiting old issues when supporting/surround facts have not changed.

LTC Michael Lanham ***is an FA53 officer and who served as the information assurance program manager at USARCENT from 2008-2009. He has served as a CNO plans officer at ARFORCYBER and JFCC-NW and deputy chief information officer at JFCC-IMD. He has bachelor's degrees in computer science and computer engineering and a master's degree in computer science.***

Thelma Wandahl-Bundesen, ***a retired U.S. Air Force lieutenant colonel and former USARCENT IA manager, is currently working as a Department of the Army civilian employee. She has 30 years experience in the communications and IT fields within DoD and NATO.***

Donald DeLaHunt, ***a retired U.S. Army veteran, is a Department of the Army civilian working as the IA manager for 160th Signal Brigade. He has 25 years of professional service to our Nation and four years directly supporting the IA initiative.***

Michael Charbonneau, ***a retired U. S. Air Force master sergeant, is a General Dynamics IT contractor and was the DIACAP subject matter expert for the 160th Signal Brigade. He has over 25 years of experience in the network and IT arenas and 18 years experience on certification and accreditation efforts.***

Acronym QuickScan

ACA – Agent of the Certifying Authority
APMS - Army Portfolio Management System
AOR – Area of Responsibility
AR – Army Regulation
ARTEP – Army Training and Evaluation Program
ATO – Authority to Operate
ASCC – Army Service Component Command
C&A – Certification and Accreditation
CA – Certifying Authority
CJCSI – Chairman of the Joint Chiefs of Staff Instruction
CND – Computer Network Defense
DA – Department of the Army
DAA – Designated Approving Authority
DISA – Defense Information Systems Agency
DoD – Department of Defense
FM – Field Manual
CA – Certifying Authority
CAP – Circuit Action Process
CCSD – Command Communications System Designator
CENTRIXS – Coalition Enterprise Regional Information Exchange System
CONUS – Continental United States
DIP – DIACAP Implementation Plan
DOIM – Directorate of Information Management
EXEVAL – External Evaluation
GCTF – Global Counter-Terrorism Force
GIG – Global Information Grid
IG – Inspector General
RCERT – Regional Computer Emergency Response Team
SC(T)(P) – Signal Command (Theater)(Provisional)
IA – Information Assurance
IAM – Information Assurance Manager
IANO – Information Assurance Network Officer
IATO – Interim Authority to Operate
IAPM – Information Assurance Program Manager
ICAN – Installation Campus Area Network
IP – Internet Protocol
IPR – In Progress Review
ISAF – International Security Assistance Force
JP – Joint Publication
MCFI – Multi-national Coalition Forces Iraq
MCP – Main Command Post
MDMP-Military Decision Making Process
MFR – Memorandum for Record
NIPRNet – Non-secure Internet Protocol Routing Network
P/C/S – Posts, Camps, and Stations
POA&M – Plan of Actions and Milestones
RNOSC – Regional Network Operations and Security Center
SIP – System Identification Profile
SIPRNet – Secure Internet Protocol Routing Network
SWA – Southwest Asia
TNOSC – Theater Network Operations and Security Center
TIG – Theater Information Grid
USARCENT – U.S. Army Central
USCENTCOM – U.S. Central Command