Chapter 5

Command and Control Protect

The user is responsible for protecting his information system and its data. By failing to implement the correct C2 protect (C2P) measures, the user can experience data loss, hardware or software damage, and compromise of data. Any or all of these can result in the degradation of mission capability or the incapacity to support the mission. This chapter covers the procedures in protecting our systems. We must understand our system's vulnerabilities and what we must do to obtain assistance in protecting, detecting, and reacting to an intrusion or security violation.

THREAT

5-1. When deployed, information systems are subject to the same threats encountered in garrison. However, some of these threats are easier to exploit because of the deployed environment. Familiarization with the following terms is essential in understanding our systems' vulnerabilities.

INTENTIONAL

5-2. This threat is a deliberate attack on a computer system's resources or its ability to process. Insider threats are still the most serious while deployed because of greater access and knowledge of system assets and safeguards. However, threats from outside increase while deployed because of closer proximity and increased vulnerability.

UNINTENTIONAL

5-3. This threat results from an accident or procedural failure. The unintentional threat could increase while deployed because of longer and higher stress levels, different working environments, or poor training.

STRUCTURAL

5-4. This threat results from flaws in the construction of the physical environment, the physical configuration, or the system or application software. While deployed, computers often will not be operated in an office environment; rather, they will be operating in tents, vans, or other uncontrolled environmental facilities.

NATURAL

5-5. This threat can result from the locale or mode of operations. A varying degree of natural threats such as earthquakes, flood, dust, temperature, and humidity vary greatly between locations and must be considered.

ATTACKS

5-6. Some attacks against information systems can have a delayed effect and others are immediate. These attacks can corrupt databases, control programs, and degrade or physically destroy information systems.

COMPUTER

5-7. These attacks are aimed at software and data contained in individual computers or against computers connected to a network. Protecting information systems has become an important and everyday task. SAs/NAs must be trained in all aspects of information systems security (ISS). They must maintain and protect information systems and their networks. The SA/NA coordinates with the ISSO and reviews audit information for detecting system abuse.

PHYSICAL

5-8. These usually involve destruction, damage, overrun, or capture of the physical components.

THEFT

5-9. This is a physical attack that does not involve destruction or damage. However, theft of items, such as cryptographic keys and/or passwords, is of a particular concern. These items could support subsequent electronic or computer attacks.

ELECTRONIC

5-10. These attacks focus on specific or multiple targets within a specified area. Jamming, signal intercept, emitter direction finding, and geolocation can degrade communications.

HIGH ENERGY

5-11. High-energy attacks are electromagnetic pulses that destroy or damage electronic devices.

C2P MEASURES

5-12. C2P can be offensive or defensive. Offensive C2P measures use the five elements of C2 warfare to reduce the adversary's ability to conduct C2 attacks. These elements are–

- Operations security (OPSEC).
- Military deception.
- Psychological operations.
- Electronic warfare.
- Physical destruction.

Defensive C2P measures reduce friendly C2 vulnerabilities from adversary C2 attack by using adequate physical, electronic, and intelligence protection. FM 100-6 further explains the elements of C2 warfare, C2 attack, and information warfare affecting information operations.

SHARED C2P-NSM RESPONSIBILITIES

5-13. Command and control protect-network security management (C2P-NSM) encompasses those measures taken to maintain effective C2 of our forces. The goal of C2P-NSM is to integrate signal operations, technical engineering, security disciplines, and intelligence (or counterintelligence) support to ensure the availability, integrity, and confidentiality of information. The C2P-NSM strategy addresses protect, detect, and react measures. Figure 5-1 shows the shared and overlapping C2P-NSM responsibilities.

Figure 5-1. Shared C2P-NSM Responsibilities

PROTECT

5-14. Everyone must protect the information network from malicious threats. These threats can intentionally unleash computer viruses, trigger future attacks, or install software programs that compromise or damage data and systems. Users who are inexperienced or untrained that cannot identify security violations are jeopardizing their systems and networks which are vulnerable to all attacks. A comprehensive training program must be a part of the unit's training.

5-15. Information systems users must be trained to identify and to protect the system against intrusions. The most common intrusions include–

- Unauthorized users (hackers).
- Insiders (individuals with legitimate access).
- Terrorists (organized groups threatening national security).
- Nonstate groups (drug cartels and social activists).
- Foreign intelligence services.
- Opposing militaries or political opponents.

C2 Strategy

5-16. The Network Security Improvement Program is the primary plan for enhancing the overall network and systems security posture for the Army. This is a protection plan for all C2/information systems. Figure 5-2 gives an example of a typical network security plan.

5-17. **External Digital Perimeters.** These perimeters consist of COMSEC, firewalls, and security guards, and, where necessary, physical isolation which serves as a barrier to outside networks such as the Nonclassified Internet Protocol Router Network (NIPRNET).

Figure 5-2. Example of a Typical Security Network Plan

5-18. **Internal Digital Perimeters.** These perimeters consist of firewalls and/or router filtering that serve as barriers between echelons and/or functional communities. Internal barriers may also use COMSEC and guards.

5-19. **Local Workstation Security.** It consists of individual access controls, configuration audit capability, C2P tools, and procedures.

5-20. **NSM and/or Surveillance.** They provide real-time network surveillance and reaction to network intrusions.

5-21. **Robust and Resilient Infrastructure.** This infrastructure can contain the damage from attacks and is readily repairable if attacked.

DETECT

5-22. C2P-NSM facilities can detect security policy violations. Selected events or occurrences (such as numerous log-in attempts within a specified period) are monitored using conventional and C2P tools. Two violations of security policies are integrity and operational.

- Integrity violations indicate potential interruptions in information flow (such as illegally modified, inserted, or deleted information).
- Operational violations indicate a requested service is unavailable, malfunctioned, or an invocation of service.

REACT

5-23. Certain events will alert users and/or managers of possible internal or external intrusions. Users must be able to detect an intrusion and react accordingly to correct the problem. This includes operating during periods of degraded operations due to hostile attacks. The users and/or managers must–

- Report the incident to their immediate supervisor and/or ISSO.
- Follow the incident security network policy as outlined in the unit SOP and other applicable security regulations.
- Restore destroyed and/or compromised data (from backups).
- Report the incident to other activities, as required.

5-24. Appropriate reactive measures are taken when problems occur. Security management encompasses the means to alert the network and/or system manager when detecting intrusion attempts. The network and/or system managers react to intrusions by–

- Changing boundaries/perimeters.
- Reconfiguring firewalls, guards, and routers.
- Rerouting traffic.
- Changing the level of encryption or rekey.
- Zeroizing communications that are suspected of being compromised.
- Reestablishing a net with selected members.
- Changing authentication/passwords.

TOOLS

5-25. Software and hardware tools help network and security managers to prevent, detect, and monitor intrusions. These tools change constantly as technology continues to improve. The current list of approved network tools is available through the Office, Director of Information Systems for Command, Control, Communications, and Computers and distributed to subordinate activities. The G6/S6/ISSO representative has the list for the latest approved C2P-NSM tools.

5-26. C2P-NSM tools–

- Audit monitoring and intrusion detection systems.
- Isolate systems under attack by automated infrastructure management.
- Detect malicious code and eradicate systems.
- Analyze and assess vulnerability.

5-27. C2P tools with or embedded within the information systems to protect against external and internal hackers and virus attacks include–

- Antivirus software.
- Hard disk purge capability.
- Network mapping software.
- Audit profile software.
- Intrusion detection system.
- Secure password generation systems.
- In-line network encryption devices.
- Firewalls, high-assurance guards, and tactical security guards.
- Encryption key management systems.
- Security posture of systems and networks.

DUTIES AND RESPONSIBILITIES

5-28. The Army C2P-NSM program management plan and AR 380-19 requires a clearly defined structure of ISS personnel. (See Appendix A.)

INFORMATION SYSTEMS SECURITY PROGRAM MANAGER (ISSPM)

5-29. The program executive officer for the command, control, and communications system is the ISSPM and is responsible for–

- Developing the security architecture.
- Coordinating and reviewing operational concepts, SOPs, and security accreditation for C2 systems.
- Ensuring certifications of individual systems are completed.
- Ensuring transient electromagnetic pulse emanations standard (TEMPEST) certifications of individual systems are IAW AR 381-14.

INFORMATION SYSTEMS SECURITY MANAGERS (ISSM)

5-30. Individual program managers or battle lab sponsors for Task Force XXI Systems perform ISSM functions. ISSMs–

- Develop the systems operational concept, security SOP, and security accreditation. These are submitted through the ISSPM for review and to the designated accreditation authority (DAA) for approval.
- Conduct individual systems risk assessment for operating their systems.
- Conduct system-specific security training and awareness programs.

INTELLIGENCE OFFICER

5-31. The brigade intelligence officer (S2) is responsible for identifying and assessing foreign intelligence threats to command assets. The S2–

- Administers the Personnel Security Program IAW AR 380-67.
- Ensures the Command Statement of Intelligence Interest (AR 381-19) registers the receipt of validated intelligence impacting on the integrity and reliability of the network.
- Assists in identifying threat factors.
- Coordinates with the national intelligence agencies.
- Evaluates C2P-NSM incidents and implements reporting procedures.

ISSO

5-32. The G6/S6 is responsible for secure operations of the information systems. Therefore, the G6/S6 oversees the functions of the ISSO.

5-33. The automation officer and/or systems integration technician in the G6/S6 signal office normally serves as the ISSO. He–

- Prepares, distributes, and maintains plans, instructions, guidance, and SOPs for C2 systems security.
- Ensures all systems have approved accreditation (operational or generic) to operate at the SECRET level in the systems high mode of operation IAW AR 380-19.
- Coordinates with the brigade S2 to ensure users have the required security investigations, clearances, authorizations, and the need-to-know.
- Establishes and implements a system for issuing, protecting, and changing system passwords.
- Implements ISS training and awareness and incorporates this training into the overall unit security and training programs.
- Monitors, reviews, and evaluates the security impact of changes and coordinates this with the ISSM.
- Directs threat and vulnerability assessments to help the commander properly analyze the risks to the information systems and interconnected systems.

USER

5-34. The user is responsible for terminal security and must–

- Secure operations of the systems.
- Operate terminals IAW appropriate procedures and local SOPs.
- Perform other duties as assigned by the ISSO, SA/NA, and the mission applications administrator.

PASSWORD CONTROL

5-35. Passwords for processing classified or unclassified material over information systems must be randomly generated. Passwords must have at least an 8-character string using the 36 alphanumeric characters with at least 2 of the characters being numeric. The ISSO or designated representative generates, issues, and controls all passwords IAW the following guidelines:

- Users will not have any control over choosing their passwords.
- Passwords are handled and stored as the most sensitive data contained in the system.
- Knowledge of individual passwords will be limited to a need-to-know basis.
- Passwords will not be shared.
- Passwords will be issued only if the user has authorization to access the system.

5-36. Individual users will be briefed on–

- Password classification and exclusiveness.
- Measures to safeguard classified and unclassified passwords.
- Prohibitions against disclosure to unauthorized personnel.
- Immediate reporting of password disclosure or misuse.

5-37. Passwords are issued only once and are retired when the time limit has expired or the user has been transferred. Passwords, as unique identifiers of individual authority and privilege, **WILL NOT** pass between individuals, even if those individuals are employed on the same project.

5-38. All passwords on classified systems are changed at least quarterly. Passwords on nonsensitive and sensitive but unclassified systems will be changed semiannually.

5-39. Passwords are inhibited, overprinted, or otherwise protected from unauthorized observation on terminals and video displays.

COMSEC

5-40. The G6/S6 has overall COMSEC responsibility. Table 5-1 outlines various COMSEC systems to protect C2 data.

Table 5-1. COMSEC Systems

System Type	Key Source/Classification	Controlling Authority/POC
SINCGARS	Electronically Generated/SECRET	G6
EPLRS	Electronically Generated/SECRET	G6
GBS/BADD KG-194	TBD/TBD	NSA
NTDR	TBD	G6 COMSEC Office
TRI-TAC/MSE	Tape Generated/TBD	NSA/Signal Battalion
Wireless LAN	TBD	TBD

INCIDENT REPORTING

5-41. The user/ISSO will log and report all violations and insecurities as shown in Table 5-2. To facilitate detection and investigation of security breaches, all devices require reporting to an audit manager or providing an audit trail. The G6/S6 evaluate local and remote incidents and report to the brigade systems integrator for evaluation and investigation, if warranted. The brigade automation officer evaluates and/or investigates security breaches, coordinates recovery actions, and assists the brigade intelligence officer in preparing reports.

Table 5-2. C2P-NSM Incident Reporting (Internal to Brigade)[1]

Incident	Precedence	Action	Information
Copyright Violation	Routine	user>ISSO	S2/S3/S6
Virus Detection	Priority	user>ISSO	S2/S3/S6
Intrusion (internal)	Immediate	user>ISSO	S2/S3/S6
Intrusion (external)	Immediate	user>ISSO	S2/S3/S6
Malicious Code	Priority	user>ISSO	S2/S3/S6
Unauthorized Monitoring	Priority	user>ISSO	S2/S3/S6
Compromise	Priority	user>ISSO	S2/S3/S6

[1] The commander will determine external brigade reporting based on staff evaluation.

EMERGENCY PROCEDURES

5-42. Procedures for protecting our networks from being compromised are carried out only after directed to do so, or under extreme emergencies. These emergencies are normally covered in the unit SOP. Methods for denying access to sensitive and to classified systems are–

- Zeroize COMSEC devices.
- Purge systems.
- Destroy classified systems, **when capture is imminent.**