Global Information Assurance Certification Paper

GIAC GSEC Practical (requirement v.1.2f)
Following ADMINISTRIVIA Version 2.0

The NSA: A Brief Examination of the "No Such Agency"

Steven H. Bennett
1 October 2001

Introduction

The National Security Agency (NSA) plays an important role in United States Information Systems (IS) security - not only as IS security relates to national security, but also in the technologies, products, and methods that are developed in the US and made available to the public. This paper introduces the NSA to the reader and discusses some of the key technologies, methods, and issues that relate to its mission.

As a former NSA contractor, I spent ten years working on NSA programs. During that time, I gained considerable insight into the workings of the agency. In writing this paper great care was taken to ensure that no classified or sensitive information was disclosed. Therefore, the depth and breadth of this paper is limited to only that information that is readily available from open sources and information that is known to be unclassified. So, if the technical depth of this paper seems in some areas to be a bit shallow, it is because presenting greater detail will approach topics that should not be discussed for obvious reasons. The section herein on Operational Security (OPSEC) sheds additional light on this issue.

This paper begins with a discussion of the background and history of the NSA. Subsequent sections present the primary missions of the NSA and discuss the key technologies involved in each. The paper continues with key topics that are of relevance to the SANS GIAC Security Essentials course: OPSEC, NSA's role in security product assurance, and NSA's role in the development and sale of commercial information security products.

Background

On December 28, 1951 James B. Lay, Executive Director of the National Security Council, commissioned a study to survey all communications intelligence activities of the US. Previous to this, the direction of communications and electronic intelligence had been the responsibility of the Armed Forces Security Agency (AFSA), however the AFSA had little power and no authority over the armed forces service units. The result of the study, know as the "Brownwell Committee Report", was a recommendation to create the National Security Agency in order to provide greater coordination and direction of communications and electronic intelligence activities at the national level.

In 1952 President Harry Truman established the NSA by Presidential directive. As an agency within the Department of Defense, the NSA has responsibility for two primary missions: information intelligence (the interception of foreign intelligence communications) and information assurance (the protection of US government communications). The NSA plans, coordinates, and directs all activities of the US armed forces related to these two missions and

provides much of the technologies, products, resources, and services used to carry out and support these missions.

The NSA is closely associated with the Central Security Service (CSS). The Director of the NSA is also the Chief of the CSS. The CSS is comprised of staff from Army, Navy, Marine, and Air Force operating elements. The CSS is in effect the coordinating agency betweenthe NSA and the armed forces. The commanding officers of each of the armed forces cryptologic organizations are subordinate to the Chief, CSS.

The NSA's role in a nutshell is to make sure that the US government understands foreign communications while protecting its own. The key component of this role is cryptography – the knowledge of which allows the government to decipher foreign intelligence and to protect its own intelligence. The NSA accomplishes this with worldwide networks of highly complex systems – both signals collection systems and secure communications systems. The NSA's challenge is to continually keep up with new technologies and continually build new systems and capabilities to keep up with the ever-changing communications, cryptographic, and computing landscape.

The NSA mission is not without controversy. If NSA can eavesdrop on foreign governments, they can also, of course, eavesdrop on US citizens. In addition, the NSA controls what kinds of security and cryptographic products can be produced and exported by US companies. These situations contribute to a feeling by some that the NSA wields great power that can be abused – the NSA as "big brother". Combine this with the fact that, due to the nature of its work, the NSA must be extremely secretive about its operations and one can see why the NSA has often come under attack by civil libertarians. However, few can argue that the success of the NSA is crucial to the defense of the United States.

Mission Examination

The two primary missions of the NSA are Information Intelligence and Information Assurance. Although separate, these two missions have a symbiotic relationship and enhance each other by the sharing of information and technologies. The following sections explore the nature and technologies related to each.

The Information Intelligence Mission

The Information Intelligence mission involves the effective and unified organization and control of foreign signals collection and processing activities. Generally, the intelligence mission is referred to as SIGINT (Signals Intelligence). SIGINT refers to all categories of intelligence information collection by electronic means including COMINT, ELINT, TELINT, and RADINT. Each are explained below:

- **COMINT** – Intelligence information obtained from intercepts of foreign communications. COMINT is the direct interception of voice or data communications transmitted by electronic means. Collection of this information includes signals searching, signals analysis, decryption, plain text analysis, and reporting.

- **ELINT** – Intelligence and technical information obtained from electromagnetic emanations from electronic equipment. All electronic equipment emits electromagnetic energy. This energy can be collected and analyzed to obtain intelligence about its source. For example, the electromagnetic energy emanating from a computer monitor can be collected and analyzed using sophisticated antennas and ELINT processing equipment to obtain the actual data being displayed on the monitor.

- **TELINT** – Intelligence and technical information obtained from the interception of foreign telemetry signals. Telemetry refers to signals and data used to control the flight and operation of aircraft and spacecraft, such as satellites. TELINT systems intercept and analyze foreign telemetry to obtain information about foreign satellite operations. Note that the intercept of the *data* to/from these satellites falls under the category of COMINT.

- **RADINT** – Intelligence information derived from the interception of foreign radar signals. RADINT is sometimes considered to be a subset of ELINT.

In general, the NSA's role in SIGINT is limited to the collection of raw intelligence. This raw information is passed on to other US government groups or agencies for further analysis, interpretation, and dissemination.

Each of the intelligence areas involves the design, production, and maintenance of sophisticated collection and analysis systems. These systems collect massive amounts of data on a daily basis. The NSA develops such systems and is also responsible for the oversight of the development of these systems by other services. The NSA provides technical guidance and defines the policies and rules for their operation, staffing, and programs.

The Information Assurance Mission

The Information Assurance mission of NSA involves the secure communication and storage of classified US government information. Information assurance protects US telecommunications from exploitation by foreign intelligence and from unauthorized disclosure. The assurance mission is termed INFOSEC (Information Security) and is comprised of COMSEC and COMPUSEC. Each are explained below.

- **COMSEC** – Communications security refers to programs, systems, and products used to ensure that transmitted information is protected from unauthorized disclosure during the communications process. COMSEC systems/equipment may be standalone or may be integrations of various cryptographic and TRANSEC components. COMSEC systems/equipment consist of four main parts:

- Cryptosecurity - The use of technically sound cryptosystems for the protection of data integrity and access control.
- TEMPEST – Stands for Transient Electromagnetic Pulse Surveillance Technology. TEMPEST technology eliminates any information-carrying electronic emanations from COMSEC equipment, thus protecting COMSEC systems from detection by foreign ELINT systems. All COMSEC hardware must be TEMPEST-approved. See the section covering TEMPEST later in this paper.
- Physical Security – The physical separation of unauthorized individuals from the source of unencrypted information
- TRANSEC – Transmission security is the component of COMSEC that involves protection of transmitted data using measures other than cryptosecurity. These measures range from simple techniques, such as frequency hopping, to highly complex transmission schemes.

- **COMPUSEC** – Computer security refers to the protection of classified data that resides in a computer. COMPUSEC covers a wide range of areas, from access control to configuration management. A computer system that has been validated to handle classified information to a known classification level is called a Trusted System. The NSA has developed the government standards for implementing and evaluating such systems commonly referred to as the Rainbow Series (thirty books, each a different color). The series consists of a requirements document called the Trusted Computer System Evaluation Criteria (TCSEC), and a series of guidelines that expand upon the requirements set forth in the TCSEC. The NSA also publishes the Information Systems Security Engineering Handbook and other guidance documents in security engineering.

The NSA accomplishes the assurance mission by overseeing the development and usage of COMSEC and COMPUSEC systems used by the US government. Any government entity that handles classified information in electronic form must use NSA-endorsed and approved COMSEC or COMPUSEC systems.

The NSA has two categories for the endorsement of COMSEC systems: Type 1 and Type 2.

- **Type 1** systems offer the highest level of security and are approved for securing classified and sensitive US government information. Type 1 systems are available to US government users and contractors and limited non-US government entities. Type 1 systems are subject to strict export restrictions. A Type 1 device is considered to be a Controlled Cryptographic Item (CCI) which means the device itself is classified and it must be properly stored, controlled, and used in accordance with strict rules.
- **Type 2** systems are approved for securing unclassified information. Type 2 systems are available to both US government agencies and the private sector.

They are suitable for protecting corporate proprietary information. Type 2 systems are also subject to export restrictions.

Key Information Assurance Technologies

The GIAC Security Essentials course covers many technologies that are related to information assurance. However, there are two technologies that are of prime interest to the NSA that are not covered by the course: TEMPEST and Red/Black Communications. If one performed all of the security measures identified in the Security Essentials course, such a system would still not be considered "secure" from NSA's standpoint. To protect US government classified information more hardening is needed. Such hardening methods are discussed below.

TEMPEST

Computers and communications equipment emit RF energy that can be representative of the information in the equipment and thus be a source of information compromise. Any electrical circuit that carries a time-varying signal will emanate electromagnetic energy. The strength of this energy is proportional to the signal's power (current and amplitude) and frequency. Since the power and frequency correlate to the information content of the signals, the emanation will bear some relationship to the data. It may therefore be possible to reconstruct the original information by analysis of these emissions. The study of the technology of compromising emissions is called TEMPEST. The term TEMPEST also refers to the countermeasures applied to equipment/systems to reduce or eliminate stray emissions that may comprise the information. All Type 1 systems (and some others – see the section on Red/Black Communications herein) must be TEMPEST-approved by the NSA.

To build a TEMPEST-approved system, the reduction of two kinds of emanations must be addressed in the design: radiated emissions and conducted emissions. Radiated emissions are RF energy that is "broadcast" into the air by the circuitry much like a radio antenna. Conducted emissions are stray RF energy that is carried in wires leading to and from the equipment. This includes both power and signal wires.

There are several techniques that are commonly used to reduce the radiated and conducted emissions and create a TEMPEST-approved system/equipment. Generally they fall into two categories: low emanation design and brute-force.

- **Low-emanation design** – While the subsequent measures to reduce emanations are good, the best approach is to design circuits that create little or no emanations in the first place. The most common method to accomplish this is low-power design. The lower the power consumption of the electronics, the lower the stray RF energy, which means less brute-force methods will be required for the system to meet TEMPEST standards.
- **Shielding** – One brute-force method of reducing radiated emissions is shielding. The equipment is literally wrapped in conductive material, forming a box that contains all the emissions within it. Sometimes entire systems are placed in

shielded rooms (called screen rooms) or even shielded buildings. Any panels or doors must be sealed with conductive gaskets that are designed and installed in accordance with strict TEMPEST guidelines.

- **Waveguides** – One problem that shielding presents is that most electronic equipment can't be completely sealed in a metal box. Openings must be present to provide airflow for cooling or to provide access to displays or controls. Such equipment can have openings in the shielding as long as the opening is constructed as a waveguide. A waveguide can be thought of as a shape or a material that, due to its physical properties, only allows energy of a particular frequency to pass through it. For instance, openings for fans are commonly covered with a honeycomb-shaped screen made of conductive material. Each hole in the honeycomb is of a shape that allows air to pass through the hole, but only certain wavelength (frequency) signals can pass through the hole due to its size. In selecting the correct type of honeycomb materials, the equipment is analyzed to determine what kinds of emanations are produced, and then the appropriate size honeycomb is chosen to reduce the targeted emanations
- **Filters** – Various kinds of electronic filters are used throughout a TEMPEST system to reduce the stray energy produced at specific frequencies. Filters are especially used on all signal and power wires connected to and from the equipment.

The NSA has responsibility for the approval and endorsement of all TEMPEST equipment used for classified information handling. the NSA has established a specific process to be followed to design, build and approve a TEMPEST equipment/system. All TEMPEST programs must start with a TEMPEST Control Plan that defines the system/equipment and sets forth the plan for implementing TEMPEST countermeasures. Next, a TEMPEST Test Plan is developed that defines the requirements and approach for TEMPEST Testing. After the equipment is built, it is subject to testing at an NSA-approved TEMPEST testing facility. During testing, the equipment is placed into special rooms that contain antennas and signal measuring equipment. The equipment is operated in real operational states and the antennas and other test equipment pick up and measure radiated and conducted emissions. Finally, a Test Report is produced which the NSA reviews in order to grant or deny equipment approval.

Red/Black Communications

The NSA views the world of communications in two categories of media: red and black. Each category refers to the type of information that can be transmitted over that media. A red communications system can handle and fully protect classified plaintext data. A black system can handle unclassified plaintext and classified ciphertext.

An example of a black communications system is the Public Switched Telephone Network (PSTN). Since the PSTN itself does nothing to protect the information that flows through it, only unclassified plaintext can be transmitted through this system. If classified information is to be transmitted over the PSTN, it must first be encrypted using

approved COMSEC. The term black information refers to unclassified plaintext and classified ciphertext.

A red communications system handles classified information in plaintext form. As a result, measures other than cryptography are used to protect the information. These measures are physical and TEMPEST. A red system is physically separated from black systems. Circuit separation and isolation methods are used to ensure that data from a red system does not end up on a black system. As an example, consider a secure facility or building that has its own red telephone system. This red system is physically and TEMPEST isolated from any black systems within the facility. In addition, the red system has no direct connection to systems outside of the facility. Users would be able to have classified conversations through this red telephone system without the need for cryptography. A facility that has a red system is known as a secure enclave.

COMSEC can be used to allow classified communications between two or more secure enclaves. In this case, the red systems protect the information within the secure enclaves and the COMSEC protects the information while it travels over the black communications medium between the enclaves.

Red systems and their implementations throughout the US government are part of NSA's TEMPEST programs and are subject to the approval of the NSA.

OPSEC

Operations Security, or OPSEC, is a "sub-mission" within the overall Information Assurance mission of the NSA. OPSEC is the process of denying potential adversaries any information about capabilities or operations by denying access to generally unclassified information. OPSEC is unusual in that it seeks to control access to *unclassified* information. One may ask, "Why deny access to unclassified information?" or conversely, "If the information is so important, why is it unclassified?" The answer is that the concept behind OPSEC is that by putting together pieces of seemingly unrelated unclassified information, one could figure out classified information. Lets look at an illustration.

A spy for a foreign country – let's say Liberia - is in a bar that is located near the NSA and overhears three men celebrating about a project that has recently proven to be a great success. After a little legwork, the spy easily discovers the names of the men (license plates, eavesdropping, striking up a conversation, etc.) In doing research, he finds that one of the men is a cryptoanalyst, another is an expert in spread-spectrum (an anti-jamming technique used in TRANSEC), and the other is a Liberian linguist. The spy knows that only one Liberian COMSEC system, the "Model X", uses spread-spectrum techniques. It just so happens that the week before, a Liberian espionage operation was thwarted for unknown reasons. The spy can now deduce that the NSA has successfully built a system that can intercept and decypher Model X messages. That is classified operations information that the spy figured out by piecing together bits of unclassified information. Now the Liberians can either discontinue the use of the Model X or thwart US intelligence by using it to transmit phony messages.

If the above illustration sounds like the use of social engineering, it is. Had the NSA employees used good OPSEC practices while in the bar, the spy could never have deduced that the NSA had broken the Model X cipher. OPSEC is in part, the invocation of countermeasures against social engineering. For years, the NSA employees were told never to divulge whom they work for. This is a good OPSEC practice (although one that led to the "No Such Agency" moniker). OPSEC is implemented with policies, procedures, and education that guide employees and organizations as to how they can adjust their conduct to prevent disclosure of information that could lead to a compromise.

The NSA is involved in two OPSEC programs, the Interagency OPSEC Support Staff and the National OPSEC Program. The NSA not only works to ensure that its own employees and contractors practice good OPSEC, but NSA also serves as "consultants" to other agencies providing OPSEC advice and services.

Product Assurance

The NSA has always believed that the design of information assurance systems requires a large product assurance component. Should a COMSEC device have a component failure or a software bug, that failure cannot allow the unauthorized disclosure of classified information. As a result, the NSA takes great steps to ensure the integrity of any information assurance product that carries classified information.

For software bug reduction, the NSA has been an industry leader in highly structured software development methodologies. The NSA was practicing SEI CMM Level 3+ [1] long before the CMM was conceived by the Software Engineering Institute. The NSA developed its own standard for structured software development called NSAM 81-2 and 81-3 (also know as DOD-STD-1703). NSAM was a highly disciplined implementation of the then military standard for software development DOD-STD-2167. It can be said that the NSAM was "2167 on steroids". NSAM defined high standards and exact procedures for all aspects of software development with an emphasis on software quality assurance, metrics, and bug reduction. In fact, one of the pioneers of software metrics was an NSA employee – Thomas McCabe. While employed at NSA, McCabe invented the McCabe Measure of Cyclomatic Complexity and went on to found his own software Quality Assurance products company. All software developed by and for the NSA was developed in accordance with NSAM in order to reduce the risk of unauthorized disclosure due to software failures.

For hardware assurance, all COMSEC/TRANSEC/INFOSEC products that carry classified information must undergo a Security Fault Analysis (SFA). An SFA is a detailed analysis of the circuitry of a system. Each component is identified and classified as to how the component may fail. For instance, a resistor can fail in two possible ways - as an open or a short. The analysis predicts what will happen to the security integrity of the system after any component or group of components fails. This is a painstaking analysis but it must be performed to ensure that no single or multiple component failure can result in the unauthorized disclosure of classified information.

NSA's Role in Public Security Products

The US government wants to make sure that US companies do not produce cryptographic

systems that other countries can use against the US. To this end, there are laws in place, such as the International Traffic in Arms Regulation, to restrict the export of cryptographic equipment. The NSA plays a key role in helping to regulate what products are approved for sale and export. The Information Assurance Directorate of the NSA manages industry outreach and endorsement programs that are in place to assist in the regulation of security products and compliance with applicable laws. Many of these activities are performed in conjunction with the National Institute of Standards and Technology as part of the National Information Assurance Program.

Through Commercial Product Endorsement Programs such as the Trusted Technology Assessment Program, the NSA approves/endorses industry products such as operating systems, database management systems and networking products intended to satisfy the Trusted Computer Systems Evaluation Criteria and information technology products evaluated against the Common Criteria for Information Technology Security Evaluation. For example, many firewall products such as Cisco's PIX and Lucent's VPN Firewall Brick are now endorsed by the NSA.

NSA's role in the regulation of cryptographic and security products is not without controversy. To meet its SIGINT mission, the NSA must ensure that US companies do not export security products that can be used by foreign adversaries to prevent the NSA from eavesdropping. For example, if a US company made a robust security product that used an encryption method that the NSA is unable to decipher, NSA certainly would not want Osama bin Laden to be able to buy that product. NSA's goal in this area is to ensure that the NSA has access to encrypted data that is produced by any product approved for export. That means companies must give the NSA the encryption keys before they can get their products approved.

The controversy is caused by the fact that legitimate private US organizations do not want this back-door into their data. First, they are concerned that the back door may be compromised; second they are concerned that the NSA may misuse this capability to eavesdrop on private organizations and individuals. Nevertheless, the NSA has sign-off authority on these products.

Summary

In the beginning, the NSA's job was easy. In 1952 the state of the art was wire-based telephones, RF communication systems, a handful of established cryptosystems and no data communication to speak of. Compare that to now. From a SIGINT standpoint, there are now hundreds of millions of potential sources of intelligence worldwide from telephones to cell phones to satellite systems to the millions of networks and hosts on the Internet. The shear amount of traffic that must be intercepted and analyzed on a daily basis is staggering. From an INFOSEC standpoint, all of these new telecommunications media increases the risk of compromise. In 1952, all the US government had to worry about was the Soviet block countries. Now, the US has threats ranging from foreign enemies to terrorists to tens of thousands of hackers. It is no wonder that the NSA now operates the world's largest computer and communications centers.

Most of the concepts used by information security professionals worldwide and many of the methods included in the Security Essentials course originated at the NSA. The NSA is indeed the father of information security and not only laid the foundation for much of the independent

security work that is done today, but also plays a major role in the regulation of information systems security products.

Recently there has been much criticism about the NSA's power and secrecy. The much publicized ECHELON program has been reported to allow the NSA to eavesdrop on anyone at anytime, and the NSA budget has been said to be totally unknown and not subject to public scrutiny. In fact, there are laws in place that govern what the NSA does, and if the NSA may overstep its authority in its SIGINT activities in certain occasions, that may be an acceptable penalty to pay given the current threat environment. NSA's budget is a matter of public record and is much less than many have reported. In reality, the NSA's annual budget is approximately the same as that of the CIA (about $4 billion). No other organization can match the NSA's SIGINT and INFOSEC capabilities and in today's volatile climate in which the threats to our national security are all too real, maybe it is better to be safe than sorry.

References

Bamford, James, Body of Secrets. New York: Random House, 2001.

Bamford, James, The Puzzle Palace. New York: Penguin Group, 1982.

Hager, Nicky. "Exposing the Global Surveillance System." 6 November 1999. URL: http://www.dis.org/erehwon/echelon.html

Proc, Jerry. "Some Common Crypto Terms." Crypto Machines. 20 August 2001. URL: http://webhome.idirect.com/~jproc/crypto/terms.html

Messmer, Ellen. "The Long, Strong Arm of the NSA." Cable News Network. 17 July 1998. URL: http://www.cnn.com/TECH/computing/9807/27/security.idg/

Messmer, Ellen. "Government Restrictions on Encryption Pose Obstacles for Internet Security." Cable News Network. 18 May 1998. URL: http://www.cnn.com/TECH/compuing/9805/19/encryption/index.html

Richelson, Jeffrey T. "The National Security Agency Declassified." 13 January 2000. URL: http://www.gwu.edu/~the NSArchiv/the NSAEBB/the NSAEBB23/

Cicelise, Major Carmaline. "Information Systems Security Office Services." URL: http://www.dla.mil/jgwi/docs/ISSO/

"National Security Agency Evaluates Cisco's PIX Firewall Solution." Cisco Systems. URL: http://www.cisco.com/warp/public/146/pressroom/1999/mar99/11.html

"National Security Agency Certifies Lucent's VPN Firewall Brick for Use in Government Agencies and Departments." Lucent. URL: http://www.lucent.com/press/0500/000524.the NSA.html

Federation of American Scientists, "NSA Budget and Personnel." National Security Agency. URL: http://www.fas.org/irp/the NSA/the NSAbudget.html

Federation of American Scientists, "TEMPEST." Intelligence Research Program. URL http://www.fas.org/irp/program/security/tempest.html

Federation of American Scientists, "Rainbow Series and Related Documents." National Security Agency. URL: http://www.fas.org/irp/the NSA/rainbow.htm

Federation of American Scientists, "Organization and Functions." National Security Agency. URL: http://www.fas.org/irp/the NSA/the NSAorgan.html

Federation of American Scientists, "The Interagency OPSEC Support Staff." National Security Agency. URL: http://www.fas.org/irp/the NSA/ioss/index.html

Federation of American Scientists, "Operations." National Security Agency. URL: http://www.fas.org/irp/the NSA/ioss/index.html

"What is Echelon?" Italysoft. URL: http://www.italysoft.com/software/interdetective.html

"Commercial Product Endorsement Programs." The National Security Agency. URL: http://www.the NSA.gov/isso/bao/cpep.htm

"Domestic Technology Transfer Program." The National Security Agency. URL: http://www.the NSA.gov/programs/tech/index.html

"National Security Agency." Central Intelligence Agency. URL: http://www.cia.gov/ic/nsa.html

Footnotes

[1]The Software Engineering Institute Capability Maturity Model is a widely accepted industry standard for software development and software process improvement. The model defines five possible levels of an organization's software capability with Level Five being the highest.