Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

NSS Vs NDS

Copyright SANS Institute
Author Retains Full Rights

AD

ForeScout

The head of a household is in a constant state of flux in seeking the well being and health for their loved ones from all possible harm and in order to accomplish this goal they seek wealth to assist in the payment for clothes, food, a home, toys, medical plan, college, vacations and for their own retirement.

As an Information Security Specialist you should also be seeking the same protection for the information systems under your purview as you would for your own family. So why do we cut corners and only provide the minimum requirements for these information systems.

A National Security Systems (NSS) as stated in Federal Information Security Management Act (FISMA) Public Law 107-347 under paragraph 3544. Federal agency responsibilities
‘‘(a) IN GENERAL-The head of each agency shall-
‘‘(1) Be responsible for-
‘‘(B) Complying with the requirements of this sub-chapter and related policies, procedures, standards, and guidelines, including-
‘‘(ii) Information security standards and guidelines for national security systems issued in accordance with law and as directed by the President;

In order to better understand the concept of what is or is not a National Security System (NSS). We will need to identify the underlining components of what a NSS is composed of. We will use the Executive Order 12958 of April 17, 1995 “Classified National Security Information” as a base document for definition of an NSS.

To start with a NSS will have to produce information: information is defined as: ‘‘Information’’ means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics’ that is owned by, produced by or for, or is under the control of the United States Government. ‘‘Control’’ means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

This early definition implies that a NSS is any federal information systems that processes, stores, transmits or receives information for the US Government prior to the information being segregated into classification levels.

Let us break the phrase National Security System into two parts National Security and System. From EO 12958 we see that the phrase ‘‘National security’’ means the national defense or foreign relations of the United States.

And that the word System is defined by NIST SP 800-37 as an Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III] - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

We are still at the point of stating in the early forms that a National Security Systems (NSS) would be any federal information system that produces information on behalf of the United States Government.

National as defined in Webster New World Dictionary as of or having to do with of a nation or with a nation.

Defense is defined as the act or power defending, or guarding against attack, harm or danger.

So we can extrapolate that National Security is the act or power of defending, or guarding against attack harm or danger of a nations foreign policy and it is information that is produced by personnel utilizing technology and housed in formidable structure or in other terms that protection of a nations assets and foreign policy against threat or possibility of attack.

Still if National Security is as stated above, what would be the cause for damage to National Security. EO 12958 also defines ‘‘Damage to the national security’’ means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

What is being said in regards to Damage to National Security is that the confidentiality, integrity and the availability (CIA) of information produced by a federal information system has been compromised to the point of unauthorized access/disclosure, unwarranted modification or not being available to those persons having a valid need to know access.

EO 12958 provides guidance in segregating Information into 3 three distinctive classification levels: Confidential (C), Secret (S), and Top Secret (TS). Although information is segregated into these three levels a fourth level of Unclassified or Sensitive but Unclassified (SBU) is not listed. This lack of classification fails to take into consideration an old phrase that the Total is equal to the sums of its parts. A well-versed intelligence analyst can analyze information that is listed as SBU and determine C, S, or even TS of data. So while we are protecting information at a higher level we are forgetting about the lesser information and exposing ourselves to undue manipulation.

The following definitions are extracts from EO 12958.
Unauthorized Disclosure is defined as:
“A communication or physical transfer of classified information to an unauthorized recipient.”

‘‘Classified national security information’’ (hereafter ‘‘classified information’’) means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Classification Levels.

(a) Information may be classified at one of the following three levels:

(1) ‘‘Top Secret’’ shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) ‘‘Secret’’ shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) ‘‘Confidential’’ shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Classification Categories.

Information may not be considered for classification unless it concerns:

(a) Military plans, weapons systems, or operations;

(b) Foreign government information;

(c) Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) Foreign relations or foreign activities of the United States, including confidential sources;

(e) Scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities; or

(g) Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

In FISMA we see these classification categories restated as:

“(2)(A) The term ‘national security system’ means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

‘‘(i) the function, operation, or use of which—

‘‘(I) involves intelligence activities;

‘‘(II) Involves Cryptologic activities related to national security;

‘‘(III) involves command and control of military forces;

‘‘(IV) involves equipment that is an integral part of a weapon or weapons system; or

‘‘(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

‘‘(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

‘‘(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

What is interesting to note here is under the classification categories: items ‘E’ and ‘G’. Both descriptions if left alone by themselves would qualify every information system with the federal government as a NSS, with the exception being the reference to national security; but remember National Security is the protection of a nation’s foreign policy and national defense as it relates to the protection of its assets against the possibility of attack or threat.

We see in the Federal Information Security Management Act (FISMA) that 2(B) provides a way out of being classified as an NSS as systems related to payroll, finance, logistics, and personnel management applications are exempt from being classified as an NSS. This exemption creates a Pandora’s box for these systems, can be more readily attacked and plundered to provide false or misleading information to us and to our allies.

It is rather ironic when you stop and consider that for an information system that processes information to be classified and segregated by functionality and then eliminated by certain restrictions in order to be listed as a National Security System. Only to find out that an NSS must be compliant with presidential directives and federal law. As for those systems that do not qualify as a National Security System what is the overall directives that they must follow considering the facts that they still follow presidential directives (Homeland Security Presidential Directive (HSPD-12) and Federal Law FISMA or Sarbanes Oxley. All federal information systems should be labeled as a National Security System and should subsequently be held liable to all laws and directives of the president.

Remember that a Designated Accrediting/Approving Authority or Authorizing Official (DAA/AO) is “Official with the authority to formally assume (DAA) responsibility for operating a system at an acceptable level of risk.” How can the Certifier[1] identify all of the risks if they have not identified all of the requirements?

[1] Certifier is the Individual responsible for making a technical judgment of the system’s compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: November 25th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Cape Town 2015	**Cape Town, ZA**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
SANS San Francisco 2015	**San Francisco, CAUS**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
HIMSS	**Boston, MAUS**	**Dec 01, 2015 - Dec 02, 2015**	**Live Event**
Security Leadership Summit & Training	**Dallas, TXUS**	**Dec 03, 2015 - Dec 10, 2015**	**Live Event**
SANS Cyber Defense Initiative 2015	**Washington, DCUS**	**Dec 12, 2015 - Dec 19, 2015**	**Live Event**
SANS Dubai 2016	**Dubai, AE**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Las Vegas 2016	**Las Vegas, NVUS**	**Jan 09, 2016 - Jan 14, 2016**	**Live Event**
SANS Cyber Defence Delhi 2016	**Delhi, IN**	**Jan 11, 2016 - Jan 22, 2016**	**Live Event**
SANS Brussels Winter 2016	**Brussels, BE**	**Jan 18, 2016 - Jan 23, 2016**	**Live Event**
SANS Security East 2016	**New Orleans, LAUS**	**Jan 25, 2016 - Jan 30, 2016**	**Live Event**
Cyber Threat Intelligence Summit & Training	**Alexandria, VAUS**	**Feb 03, 2016 - Feb 10, 2016**	**Live Event**
SANS Scottsdale 2016	**Scottsdale, AZUS**	**Feb 08, 2016 - Feb 13, 2016**	**Live Event**
SANS Secure Japan 2016	**Tokyo, JP**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS Munich Winter 2016	**Munich, DE**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS McLean 2016	**McLean, VAUS**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
ICS Security Summit & Training	**Orlando, FLUS**	**Feb 16, 2016 - Feb 23, 2016**	**Live Event**
SANS Secure India 2016	**Bangalore, IN**	**Feb 22, 2016 - Mar 05, 2016**	**Live Event**
SANS Anaheim 2016	**Anaheim, CAUS**	**Feb 22, 2016 - Feb 27, 2016**	**Live Event**
ICS410 London 2015	**OnlineGB**	**Nov 30, 2015 - Dec 04, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**