

Pre-Publication Review Of Web Site Content

With all its many benefits, the Internet can also do a great deal of harm if not used properly. Information on the Internet that may be intended for a limited audience is actually available to a world wide audience. The World Wide Web was not designed with security in mind, and unencrypted information is at high risk of compromise to any interested adversary or competitor. It is very easy to search the web and put together related pieces of information from different sites. For example, the search engine www.searchmil.com specializes in indexing sites with a .mil domain name. It claims (as of August 2001) to have indexed over 1 million pages of military sites, with the number of pages still growing rapidly.

Department of Defense (DoD) has been among the first government departments to take the lead in spelling out rules for what should and should not go on a web site and how information should be reviewed before it is posted on a web site. The DoD policy, cited under [Reference](#) below, should be reviewed prior to posting DoD or DoD-controlled information to a web site. This policy applies to all unclassified DoD web sites and to review and approval of requests received from DoD contractors and subcontractors or other U.S. Government agencies to post DoD information on their web sites.

DoD guidelines take into account what security access controls, if any, are in effect for the site, the sensitivity of the information, and the target audience for which the information is intended.

Briefly, most types of sensitive unclassified information discussed in this module may not go on a web site unless that site is protected by encryption. In other words, DoD Technical Information, For Official Use Only information, export-controlled information, Unclassified Nuclear Information, and Privacy Act information may not be posted on an unencrypted web site. Decisions on the handling of proprietary or trade secret information in the private sector are made by the owners of that information.

DoD guidelines also require that judgments about the sensitivity of information take into account the potential consequences of "aggregation." The term "sensitive by aggregation" refers to the fact that information on one site may seem unimportant, but when combined with information from other web sites it may form a larger and more complete picture that was neither intended nor desired. In other words, the combination of information from multiple web sites may amount to more than the sum of its parts. Similarly, the compilation of a large amount of information together on one site may increase the sensitivity of that information and make it more likely that site will be accessed by those seeking information that can be used against us.

The following table from the DoD guidance on reviewing web sites¹ has been modified to fit into a smaller space. The table is a guide to determining an acceptable level of risk, but the listed types of access controls are not necessarily the only options available for protecting information.

<u>If access control is:</u>	<u>the vulnerability is:</u>	<u>and information can be:</u>
Open – no access limitations, plain text, unencrypted.	Extremely high. Subject to worldwide dissemination and access by everyone on the Internet.	Non-sensitive, of general interest to the public, cleared and authorized for public release. Worldwide dissemination must pose limited risk even if information is combined with other information reasonably expected to be in the public domain.
Limited by Internet domain (e.g., mil, gov) or IP address. Plain text, unencrypted.	Very high. This limitation is not difficult to circumvent.	Non-sensitive, not of general interest to the public although approved and authorized for public release. Intended for DoD or other specifically targeted audience.
Limited by requirement for User ID and password. Plain text, unencrypted.	High. Still vulnerable to hackers, as User IDs and passwords can be compromised if encryption is not used.	Non-sensitive information that is appropriate only for a specific targeted audience.
User certificate based (software). Requires PKI encryption through use of secure sockets layer.	Moderate. This provides a moderate level of secure access control.	Sensitive unclassified information, and information that is "sensitive by aggregation."
User certificate based (hardware). Requires PKI encryption	Very low vulnerability.	Sensitive unclassified information, and information that is "sensitive by aggregation" where extra security is

Before putting any information on a web site, you must consider how an adversary or competitor might use that information to target your organization's personnel or activities. This requires applying risk management concepts to balance the benefits gained from using the Internet against the potential security and privacy risks created by having that information available to a worldwide audience.

There are several common mistakes that people make when deciding what to put on a web site. One is to ignore the danger associated with personal data on the Internet. Another is to assume that information is not sensitive just because it is not marked with any sensitivity indicator. A third is that people underestimate the ease and potential significance of "point-and-click aggregation" of information.



Inclusion of information about home addresses or family members in biographic summaries is one of the most common errors. Personal information that could facilitate criminal, harassment, or terrorist activity against military personnel or government or defense contractor employees should not be on the Internet. This includes home address, telephone numbers other than those readily available to the public, social security number, date of birth, and any identifying information at all about family members.

For Official Use Only information and other sensitive information is normally marked with a sensitivity indicator at the time it is created. However, the absence of any sensitivity marking is not a valid basis for assuming that information is non-sensitive. Before putting unmarked information on a web site, it must be examined for the presence of information that requires protection and qualifies as exempt from public release. Don't depend on your memory or general impressions when trying to make this determination. Check the appropriate classification guide or regulation or ask a knowledgeable person.

People who have not themselves developed strong skills at searching the Internet generally underestimate the amount and nature of the information that can be found there and the ease with which it can be located. The vast quantity of information on the Internet, combined with powerful computer search engines, has spawned sophisticated "data mining" techniques for the rapid collection and combination of information from many different web sites. Very little know-how is needed, as the tools of the Internet have been designed to do this. A single user sitting at a computer in a foreign country can now identify, aggregate, and interpret information available on the Internet in ways that sometimes provide insights into classified or sensitive unclassified programs or activities.

Information relevant to operations security ([OPSEC](#)) is a particular concern. Commanders and program managers responsible for OPSEC need to identify what needs to be protected and then take a "red team" approach to how outsiders might obtain unauthorized knowledge. As a double check, military reserve units have been tasked to conduct ongoing operations security and threat assessments of DoD web sites.

One useful tool is to do your own keyword search on the Internet to learn what related information is already out there that others might use to deduce information about your sensitive activity. As you visit these other sites or read newsgroup messages, see if they have information that could be used in conjunction with your information, or with information from some other site, to deduce your sensitive information.

For example, seemingly non-sensitive technical data, when associated with a specific research or development program, might provide clues to a new weapon's capabilities, vulnerabilities, or intended uses. Similarly, unclassified and seemingly innocent information on things such as personnel travel, commercial support contracts, changes in unit deployment or training, changes in communications patterns, messages between soldiers and family members, supply and equipment orders or deliveries, etc., might, when combined with other information, provide a tip-off to sensitive plans and intentions.

Related Topics: [Pre-Publication Review](#), [Computer Vulnerabilities](#), [Operations Security \(OPSEC\)](#), [DoD Technical Data](#), [For Official Use Only and Similar Designations](#).

Reference

1. "Web Site Administration Policies and Procedures, November 25, 1998, Office of the Assistant Secretary of Defense (C3I). Approved by the Deputy Secretary of Defense December 7, 1998. The full document is available on the Internet at www.defenselink.mil/webmasters/dod_web_policy_12071998_includes_amendments_from_04262001.html

Please read the [Security and Privacy](#) and [508 Accessibility](#) Notice

This page was last updated on: November 28, 2001