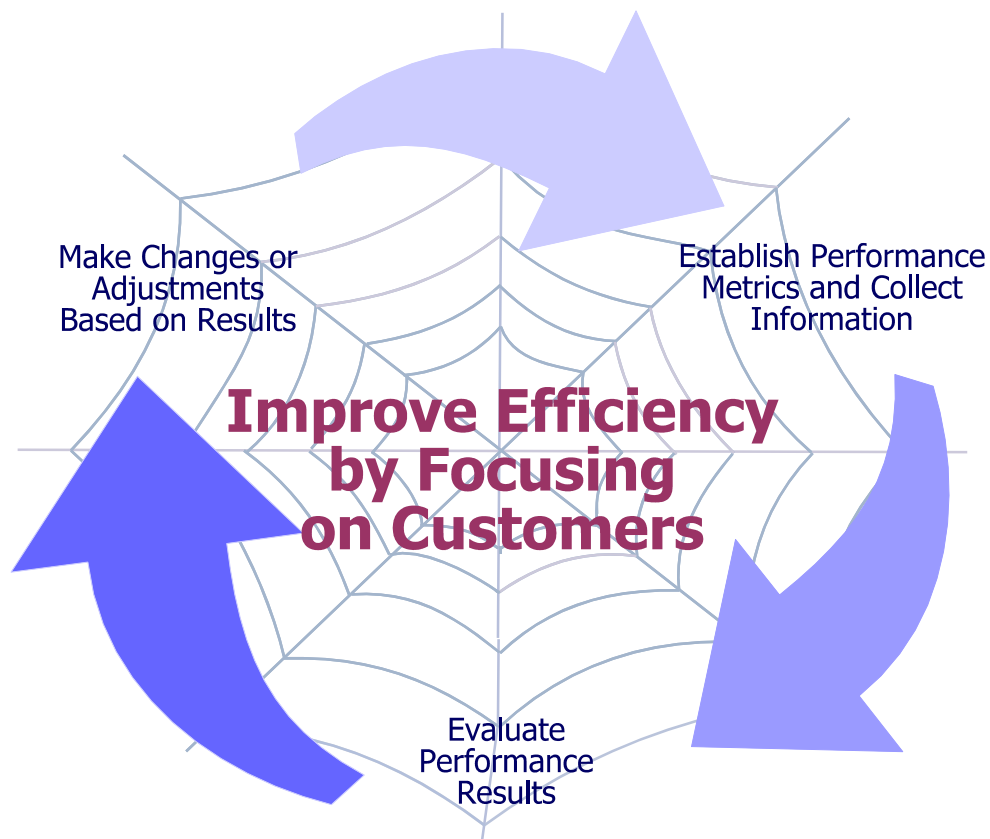




U.S. DEPARTMENT OF THE INTERIOR OFFICE OF INSPECTOR GENERAL

EVALUATION REPORT

MOVING TO A CUSTOMER-CENTERED WEB PRESENCE





United States Department of the Interior

Office of Inspector General

134 Union Boulevard, Suite 510
Lakewood, Colorado 80228

7430

June 9, 2003

Memorandum

To: Chief Information Officer, Department of the Interior

From: Diann Sandy 
Manager, National Information Systems Office

Subject: Evaluation Report on Moving to a Customer-Centered Web Presence
(Report No. 2003-I-0051)

The subject report presents the results of our evaluation of the Department of the Interior's (DOI) management and control of its Web sites. Although DOI has made some recent improvements, much remains to be accomplished. Specifically, the Department needs to manage its Web sites more efficiently, cost-effectively and securely; adhere to Federal laws and regulations; and focus on its customers.

We identified a framework for improvement based on practices employed by other Federal and state agencies as well as standards established by the Office of Management and Budget, the National Institute of Standards and Technology, and industry. We recommend that DOI implement a plan, using the framework described in this report, to improve management of its web sites. Please provide a written response to the report by July 15, 2003.

The legislation, as amended, creating the Office of Inspector General requires that we report to the Congress semiannually on all reports issued, actions taken to implement our recommendations, and recommendations that have not been implemented.

We appreciate the cooperation provided by all DOI staff during our evaluation. If you have any questions regarding this report, please call me at (303) 236-9243.

MOVING TO A CUSTOMER-CENTERED WEB PRESENCE

TABLE OF CONTENTS

CHALLENGES FACING THE DEPARTMENT OF THE INTERIOR	1
NUMBER OF WEB SITES NOT CONTROLLED	1
SECURITY NOT ADEQUATE.....	6
WEB SITES NOT COMPLIANT WITH FEDERAL LAWS AND REGULATIONS	8
WEB SITES NOT FOCUSED ON CUSTOMERS	9
BUILDING ON DOI’S EFFORTS.....	13
WEB PRESENCE ACTIVITIES	13
MORE NEEDS TO BE DONE	14
FRAMEWORK FOR IMPROVEMENT	15
STARTING THE MANAGEMENT AND CONTROL PROCESS	15
MOVING TO A CUSTOMER-CENTERED WEB PRESENCE	17
ENHANCING SECURITY	21
RECOMMENDATION	22
APPENDICES	
APPENDIX 1, EVALUATION SCOPE AND METHODOLOGY	23
APPENDIX 2, DIAGRAM OF THE DEPARTMENT OF THE INTERIOR’S WEB PRESENCE	25
APPENDIX 3, DEPARTMENT OF THE INTERIOR’S “OTHER” WEB SITES.....	27
APPENDIX 4, SCORECARD OF THE DEPARTMENT OF THE INTERIOR’S WEB SITES	28
GLOSSARY OF TERMS USED	31

MOVING TO A CUSTOMER-CENTERED WEB PRESENCE

CHALLENGES FACING THE DEPARTMENT OF THE INTERIOR

The Department of the Interior (DOI) needs to take charge of its Web presence (use of the Internet through World Wide Web technology and commonly referred to as the Web) to:

- Control the current unmanaged growth of Web sites;
- Reduce security risks;
- Comply with Federal requirements such as those governing privacy; and
- Focus on its customers - citizens, businesses, other government entities, and internal users.

NUMBER OF WEB SITES NOT CONTROLLED

DOI needs to reign in the proliferation of its Web sites to assure that Web site content and information are coordinated among bureaus and offices to minimize duplication, inconsistency, and redundancy of information. We found that DOI does not have a comprehensive inventory of its Web sites or of other components of its Web presence. (See Appendix 2 on page 25 for a diagram of DOI's Web presence). Using software (Web crawler) that automatically fetches Web sites, we estimated that DOI currently has approximately 31,000 Web sites presenting between 3 to 5 million pages of information. Figure 1 shows the percentage of Web sites maintained by major components of DOI. Appendix 3 on page 27 provides information on the sites classified as Other DOI Web Sites identified in Figure 1.

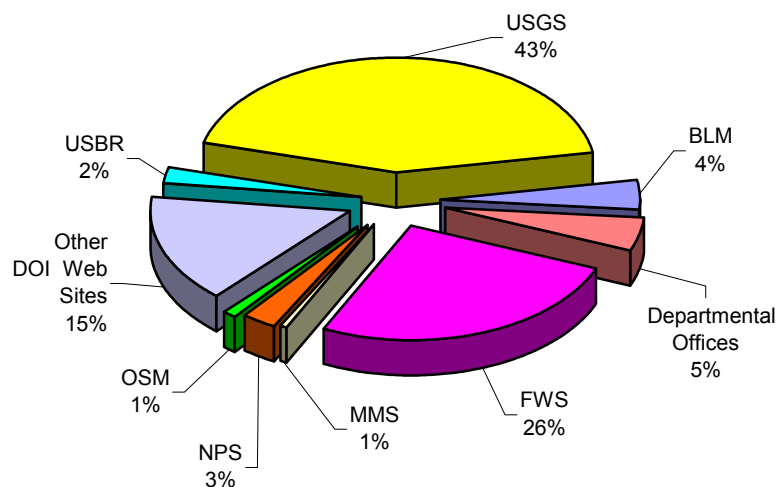


Figure 1. Distribution of DOI's Web Presence.

To provide a sense of DOI's Web sites and pages, we mapped, using a Web crawler, a portion of DOI's home page and site, as shown in Figure 2.

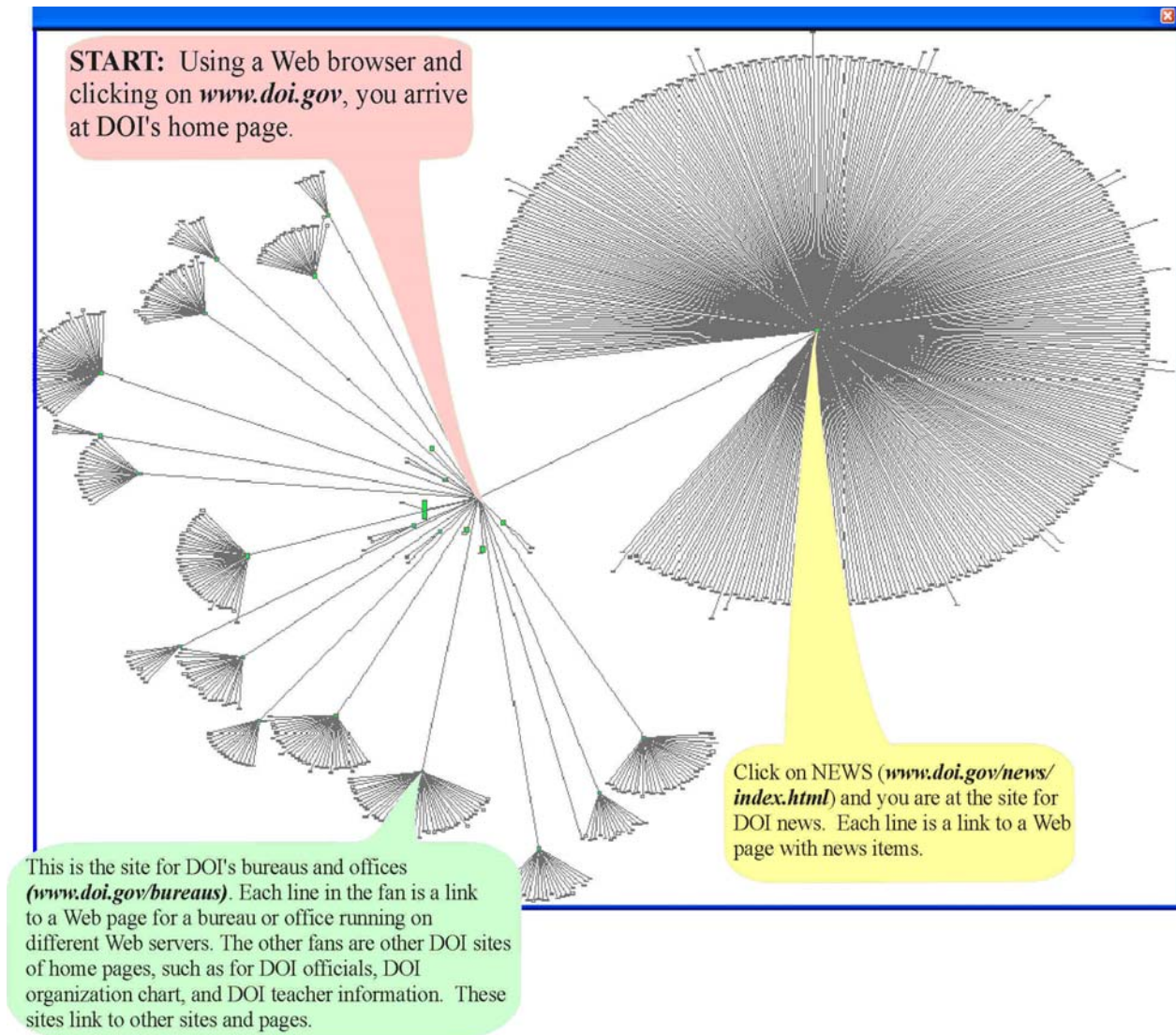


Figure 2. Snapshot of a Portion of DOI's Web Presence.

**ANNUAL SPENDING
ESTIMATED BETWEEN
\$110 MILLION TO
\$220 MILLION**

We researched industry standards and practices and analyzed the cost of current DOI contracts for outsourcing and maintaining Web sites to develop our cost estimate for annually maintaining DOI's Web presence. Our research of industry indicated that the average cost to operate and maintain a Web site is generally between \$100,000 to \$200,000 annually. The \$100,000 cost is for basic sites that have no supporting database, limited storage requirements, few individuals posting to the Web, and one domain¹. The average cost increases to \$200,000 annually based on the complexity of the site and the numbers of individuals posting information. For extremely complicated sites, the costs could reach \$500,000. These figures include the costs of acquiring:

- Information technology resources, such as computer hardware and software, necessary to operate and secure Web sites and internal networks.
- Human resources needed to design, maintain, and control Web site content and information and to manage Web-related hardware and software.

Costs for DOI contracts ranged from \$55,000 annually (for managing content, interfaces to other Web sites, and access to a third-party Web server) to \$200,000 (for content management for mapping and geographic information capabilities and databases). DOI's contracts did not always include costs for hardware and software to operate its Web sites.

We conservatively estimated, based on 1,100 domains, that DOI's annual cost to operate and maintain its Web presence is \$110 million. Using a less conservative basis of \$200,000 per domain, DOI's annual cost could be as high as \$220 million.

**CONTENT NOT
CONTROLLED**

DOI has an excessive amount of duplicated, inconsistent, outdated, and redundant information on its Web sites. For example:

- On the Office of Aircraft Services Web site, *www.oas.gov*, chapters of the Departmental Manual, Code of Federal Regulations, and Office of Management and Budget circulars, bulletins, and memoranda are duplicated rather

¹ A domain is a set of network addresses that is organized in levels. The top level identifies purpose commonality (for example, the organization that the domain covers such as ".gov"). The second level identifies a unique place within the top level domain and is equivalent to a unique address (such as "*doi.gov*") on the Internet. Lower levels on the domain may also be used (such as "*smis.doi.gov*").

than the Office of Aircraft Services creating links to the sites that maintain these documents, such as DOI's Web-based electronic library (<http://elips.doi.gov>).

- On a Bureau of Land Management's Web site, inconsistent information is provided to customers on the procedures to apply for adopting a wild horse or burro. On one Web page, the customer is informed that the application form could be downloaded, printed and completed, and mailed to the appropriate Bureau office or that the customer could apply online for adopting a horse or burro using the Internet. On another Web page, the customer is informed that he or she would have to contact the applicable Bureau field office to request the application form.
- We found that DOI Web sites were out dated or did not indicate whether the site was actively maintained, therefore not assuring that the information presented is current and relevant. For example, 8 sites had not been updated for more than a year and 27 sites did not indicate the date the site was last updated.
- Redundant information on the same DOI activities is located on numerous DOI Web sites and pages. We performed key word searches on bureaus' and offices' Web sites of selected activities that were identified on DOI's home page. The analysis, as presented in Figure 3, showed that information on the same topic is presented on hundreds and thousands of Web sites by the seven major bureaus and offices.

DOI BUSINESS ACTIVITY	Number of Sites and Pages by Bureau With Information on the Same Activity						
	OSM	MMS	USGS	BOR	NPS	BLM	FWS
Endangered Species	125	103	1,154	294	1,000+	3,776	1,000+
Fisheries	0	0	2,892	287	892	2,096	1,000+
Habitat Conservation	0	0	288	13	42	421	1,000+
Wildlife	384	209	87,063	701	1,000+	14,942	1,000+
Plants	204	312	25,978	760	1,000+	4,554	1,000+
Ground Water Resources	15	3	48,271	32	49	0	0
Water Supply	149	10	4,755	1,260	683	417	748
Water Reclamation and Reuse	5	0	5	45	10	2	20
Oil and Gas	50	530	3,422	0	298	6,431	872
Petroleum	35	238	5,283	64	363	855	445
Helium	0	0	598	0	52	201	0
Hydroelectric	0	0	1,031	547	315	109	356
Renewable Energy	0	0	49	7	98	72	23
Energy Resources	37	44	2,012	5	74	206	45

Figure 3. Results of Queries on Bureaus' and Offices' Web Sites.

PROFESSED

INFORMATION NOT ALWAYS AVAILABLE

Web sites and links were not available as presented. For example:

- Web sites that were no longer accessible by the customer were not removed. For example, instead of being linked to the selected information, customers visiting www.doi.gov/searchall.html were informed that the Web site was no longer available and to notify a Web master of the problem. Although we brought these problems to the attention of Web masters, such as webteam@nbc.gov, links to these Web sites were not removed.
- Links to Web sites resulted in the customer receiving notice that the site could not be found. For example, on DOI Web site, www.doi.gov/business, we were not able to access five Web sites under the National Business Center.

We believe these problems can be attributed to the fact that DOI has inadequate and inconsistent configuration and content management controls. We noted that DOI has not assigned responsibility for managing Web content to ensure that information is properly and consistently presented and that information is not duplicated.

Further, we found that there was limited coordination between Web site managers to ensure that links to other Web sites and pages were available and for periodically testing linked Web sites for availability.

SECURITY NOT ADEQUATE

DOI does not have adequate security to safeguard its Web presence and its networks. We ascribed this condition to the lack of uniform Web security policies, procedures, and controls and the lack of standard configuration management. This increases DOI's security risks. For example, we found that:

- Individuals could identify network devices from the Internet by using readily available network surveying software tools. This increases the ability of individuals to compromise these devices and obtain unauthorized access to DOI's networks. For instance, using one of these tools, we identified the following devices in three of the Bureau of Land Management's networks:
 - 2 Web servers
 - 2 E-mail servers
 - 6 firewalls
 - 12 File Transport Protocol servers
- Web sites maintained by or for third parties did not have adequate security safeguards. DOI has no specific policy or control technique for outsourcing or hosting Web sites or restricting the registration of domains outside of the government domains (".gov" or ".fed.us"). When DOI sites are hosted on third party networks or when DOI hosts third parties' Web sites, there is little assurance that an interconnection between the third parties' networks and DOI's networks is not created. Security risks increase under these types of arrangements and should be mitigated through safeguards specified in contractual agreements. We identified:
 - Web sites that were hosted by commercial third parties and were not within the government domains. For example, a National Park Service Web site, www.windowsintowonderland.org, is hosted on a commercial third-party's server. In addition, the site was not under DOI's control because the site was not operating on a DOI IP (Internet Protocol) address.

- Web sites that were hosted by commercial third parties and were within the government domains did not have contractual agreements. As such, DOI lacks assurance that its Web sites were protected from access from the multiple other Web sites that were operating on the third-party's server. For example, Bureau of Land Management's "Adopt a Horse" Web site, www.adoptahorse.blm.gov, was managed by a contractor and was hosted on a third-party's server but a contract did not exist for the hosting services.
- DOI was hosting Web sites for not-for-profit organizations, which may not be bound by the same security requirements as the Federal Government. For example, the Bureau of Reclamation hosted the Platte River Endangered Species Partnership (www.platteriver.org) and the Geological Survey's Northern Prairie Wildlife Research Center hosted six not-for-profit sites including the North American Reporting Center for Amphibian Malformations (www.npwrc.usgs.gov/narcam). This increases the risk to DOI's networks because third parties have access to update their Web sites.
- DOI was posting sensitive information on its Web sites. For example, the Minerals Management Service had information related to vulnerabilities of Supervisory, Control and Data Acquisition systems for offshore oil and gas production.
- Numerous types of Web server software with various versions and updates were operating throughout DOI. This increases the risk to DOI networks because known vulnerabilities in older versions of the software may not have been mitigated. Also, it creates inefficiencies in configuration management because each Web server's software must be individually evaluated, tested, and updated. In addition, DOI's ability to consolidate servers for central management and control may be inhibited because of these differences. Using network-surveying tools we identified that DOI has approximately 500 Web servers. We also obtained information on 405 of these servers indicating that DOI has at least three major types of Web server software with multiple versions of each type, as shown in Figure 4.

Apache	Microsoft IIS	Netscape-Enterprise Server
Current Version: 2.0.45 Versions Installed	Current Version: 5.0 Versions Installed	Current Version: 6.1 Versions Installed
1.1.1 1.3.26	3	2*
1.2.5 1.3.27	4	3.6**
1.2.6 1.3.9	5	4
1.3.11 1.3a.1		4.1
1.3.12 1.3b6		6.0
1.3.17 2.0.39		
1.3.19 2.0.40		
1.3.20 2.0.42		
1.3.22 2.0.43		
1.3.23 2.0.44		

Figure 4. Sample of Web Server Software Installed on DOI Web Servers.

- DOI Web server configurations (file structures) could be mirrored using network-surveying software, such as a Web crawler. This is a problem because information on Web server configuration allows an individual to easily determine specific vulnerabilities and launch attacks against Web sites. In addition, it allows Web files that were not intended to be used by customers to be at risk of disclosure and misuse.

WEB SITES NOT COMPLIANT WITH FEDERAL LAWS AND REGULATIONS

DOI's Web sites do not always comply with Federal laws and regulations pertaining to the privacy of its customers and accessibility to information by persons with disabilities. For example, we found that:

- At least one Web site (pages *www.blm.gov/nstc/soil/Kids/adopt.html* and *www.blm.gov/nstc/soil/Kids/gallery.html*) was not in compliance with the Children's Online Privacy Protection Act [15 U.S.C. Chapter 91 § 6502]. Specifically, the site did not require children under the age of 13 to obtain parental consent before submitting requested personal information.
- Three Web sites that issued persistent cookies (small Web server files stored on customers' computers) had no documented approval for use of these cookies, and only one of these sites disclosed the use of persistent cookies.

- Eight of the nine primary access points (DOI and bureaus home pages) do not meet all the requirements of Section 508 of the Rehabilitation Act Amendments of 1998 [29 U.S.C. § 794 (d)]. These requirements include providing access to electronic information to employees and other individuals with disabilities.

WEB SITES NOT FOCUSED ON CUSTOMERS

DOI's Web sites, with some exceptions, do not focus on its customers and do not allow them easy access to DOI information and opportunities. We evaluated 70 DOI Web sites to determine whether they applied best practices in 34 customer service areas covering user help features such as search and index, service navigation features including maps and events, and other user-friendly attributes such as the capability to E-mail the Webmaster. We concluded that overall DOI Web sites were adequate for 11 features, in need of improvement for 12 features, and inadequate for 11 features (see Appendix 4 on page 28 for details).

We also compared DOI's home page with the Department of Health and Human Service's (HHS) home page. This comparison, Figures 5 and 6, demonstrates the difference between a Web presence that is bureaucracy-centered (what the government does – DOI) and one that is customer-centered (what the government can do for the customer – HHS).

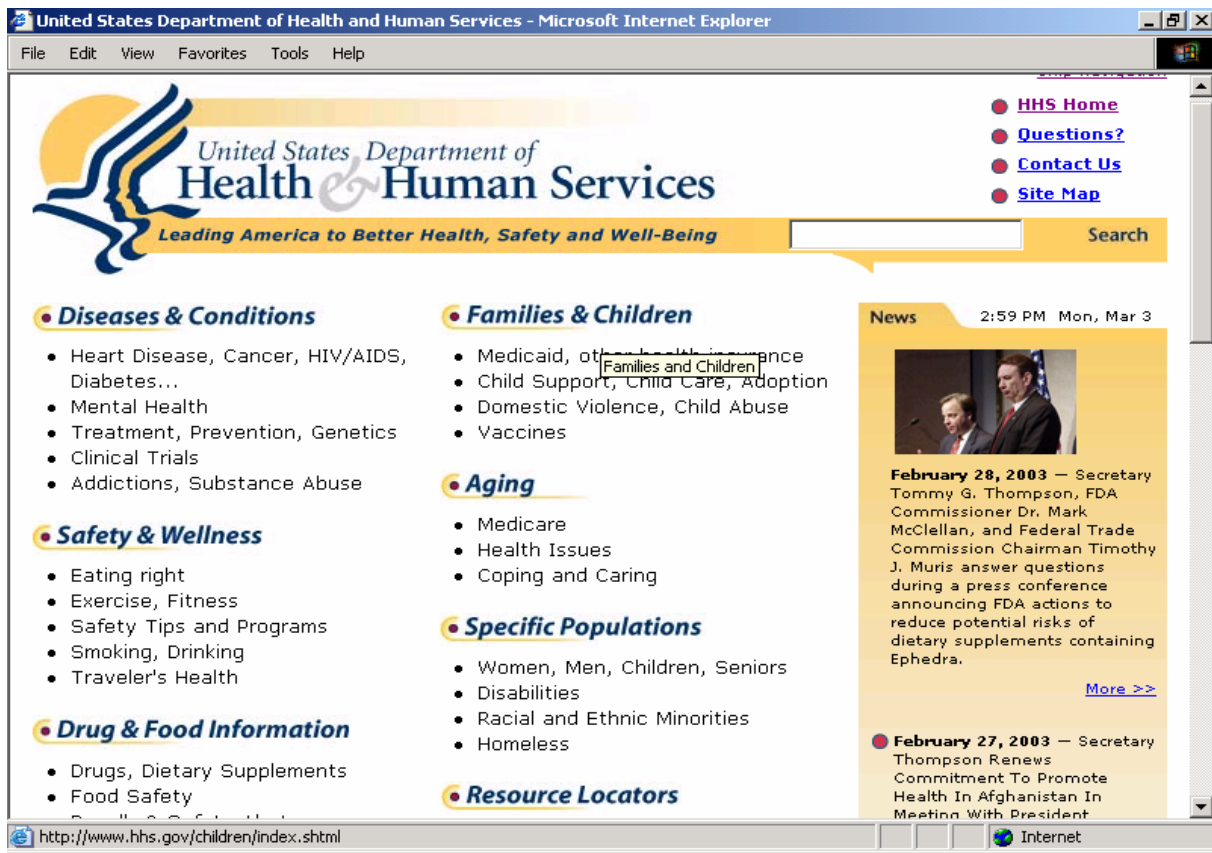
BUREAUCRACY-CENTERED



DOI-focused	The site is organized by agency function and centers on what DOI does rather than what it can provide to its customers. DOI's services and opportunities cannot be located easily on its home page.
Complicated Web Site Presentation	DOI's home page is appealing but not functional for the customer. The tab pointer links (for example "Endangered Species") provide helpful information, but not specific information on the services and opportunities provided throughout DOI. In addition, the mission of DOI is not easily found.
Slow Web Site Accessibility	The home page was not designed with customers using 56K modems for Internet access. The home page takes more than a minute to download using a 56K modem connection because of the extensive use of graphics.
Complex Search for Information and Services	Extensive knowledge and effort is needed to search for information using DOI's search function because it is limited to only bureaus' primary domains, such as <i>nps.gov</i> , <i>usbr.gov</i> , and <i>usgs.gov</i> . Much information exists in other DOI domains that do not contain the bureaus' acronyms (for examples see Appendix 3 on page 27). Also, the search function is only located on the home page. The customer is unable to perform a search from any of the other links on the home page. Rather, the customer must go back to the home page to perform the search.

Figure 5. Department of the Interior's Home Page (Bureaucracy-Centered).

CUSTOMER-CENTERED



Customer-focused

The site is organized by areas of interest to the customer and the services provided. HHS news releases are also included on the home page, but they are not the focal point of the site.

Functional Web Site Presentation

The home page is professional and conveys a business-like approach by focusing on the customer. The home page has a standardized design that includes its logo, mission, and navigation features, such as ability to ask questions and a site map.

Fast Web Site Accessibility

The home page downloads in less than 15 seconds using a 56K modem because of the limited use of graphics.

Easy Search for Information and Services

The search function is a standard feature on the top of the home page. It allows the customer to perform a search on all HHS domains. There is also an extended search function that allows the customer to narrow down a search of frequently asked questions by specific areas of information and services, such as Aging and Diseases and Conditions.

Figure 6. Department of Health and Human Services' Home Page (Customer-Centered).

BUILDING ON DOI'S EFFORTS

The goals of the President's *Expanding Electronic Government* (E-government) *Initiative* are to add value to customers' experiences with government and for government to better serve customers' needs while improving government efficiency. A key to accomplishing these goals is use of the Internet through World Wide Web technology. The purpose of a Web presence is to use Web-based resources cost effectively, deliver high-quality services, meet the needs of customers, comply with policies, and help accomplish missions and objectives. In the 1990s, the "World Wide Web" was released, and since then, the number of Web sites has grown exponentially, from an estimated 600 sites in 1993 to a million in 1997 and the number of sites continues to grow.

WEB PRESENCE ACTIVITIES

IMPROVEMENTS BEING MADE

Improvements by DOI include:

- Formalizing an E-government strategy team made up of senior level managers from the various program areas throughout DOI, Bureau and Office Chief Information Officers (CIOs), and field managers. The purpose of the team is to lead DOI's transformation to a customer-centered electronic service delivery provider, in accordance with customer and industry expectations, by using information technology (IT) to enable mission accomplishment, and to develop an E-government Strategic Plan.
- Addressing Web and electronic government requirements of the future in its Interior Enterprise Architecture.
- Beginning to consolidate Web servers and reducing the numbers of Internet access gateways.
- Implementing its policy requiring that all Web servers be contained in a Demilitarized Zone (DMZ).
- Issuing policies to improve its IT security practices.
- Initiating projects to consolidate the access to information on some DOI Web sites to better provide opportunities to customers.

- Considering the initiation of a project to implement a content management system.

SOME WEB SITES PROVIDE EASY ACCESS TO INFORMATION

We found that some of the DOI's Web sites have features which allow customers to easily locate specific information or to query for information through various techniques. For example, the U.S. Fish and Wildlife Service's home page allows the customer to select news articles by date and subject, the Bureau of Reclamation has a similar feature to aid customers in locating specific Reclamation manuals, and the Bureau of Land Management allows customers to submit requests and questions to the Bureau's Web team through a variety of electronic methods.

MORE NEEDS TO BE DONE

Despite these efforts, we believe that DOI needs to redesign its Web presence to focus on the customer, enhance security, maintain privacy, reduce duplication, and, at the same time, better manage its costs. To aid DOI in this endeavor, we developed and presented in the next section of this report a framework for improvement based on best practices identified through our reviews of various Federal and state agencies' Web sites; Federal agencies' Web procedures and practices; and Office of Management and Budget, National Institute of Standards and Technology, and industry standards.

FRAMEWORK FOR IMPROVEMENT

Our framework is based on a more centrally controlled and managed Web presence and focuses on ways for DOI to enhance its processes to not only improve its management of costs and security but also to aid in transforming its bureaucracy-centered Web presence to a customer-centered Web presence.

STARTING THE MANAGEMENT AND CONTROL PROCESS

GETTING STARTED

Inventory Web resources, justify domains and sites, and implement management controls over these resources. To accomplish these tasks, we suggest that DOI:

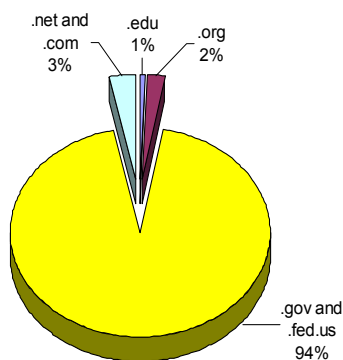


Figure 7. Distribution of DOI's Web Presence by Domain Type.

Six percent of DOI's Web domains are not government domains.

- Inventory IP addresses, Web domains and sites, and Web server operating systems and record the physical location of these resources. To help accomplish the inventory, DOI should issue a moratorium on new Web domains and sites except for urgent business reasons.
- Discontinue use of *.org*, *.net*, *.com* or other non-government domains where possible. If there is a need to use non-government domains, these should be supported by a business case and formally approved by the DOI CIO.
- Implement contracts for maintaining all outsourced and hosted Web sites and ensure that the contract language adequately addresses security requirements, including requirements to use DOI IP addresses, ensure that DOI's Web content is protected, and make sure that system configurations are consistent with DOI security policies and practices.
- Establish a position for and select a DOI Web Master. The position should report directly to the DOI CIO. The position's authority and responsibilities should include issuing and enforcing DOI policies and standards related to Web resources, such as approving all new Web domains, coordinating selection of content management software solutions and portal technologies, and Web server configuration.

- Require network management staff to coordinate with the DOI Web Master when assigning IP addresses for Web domains.
- Establish a position for and select a DOI Content Manager. We believe this position should be located within the Immediate Office of the Secretary to ensure DOI's Web sites appropriately present the Secretary's message. In addition, this position should issue and enforce policies to control the format and style of DOI Web sites, to establish an approval process for content published on Web sites, and to control the numbers of Web pages. This individual should have the authority to disable and remove pages from public access and manage information in accordance with DOI records policies. The Content Manager should also act as liaison between the DOI Web Master and all levels of program managers.

NEXT HURDLES

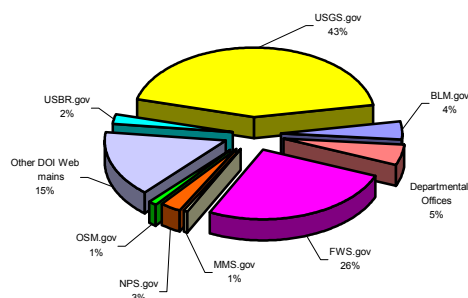


Figure 8. Distribution of the Known 1,100 DOI domains.

Fifteen percent of DOI's domains do not reside within DOI and Bureau/Office specific domains.

- Determine the need for all existing domains, Web sites, and Web pages and disable those that are not needed, not functional, or not accessible. Information on the Web should be based on the DOI enterprise lines of business. All DOI Web sites should be justified by business cases that include supporting metrics.
- Develop and implement DOI policies and standards to establish minimum controls for its Web presence. These policies and standards should ensure compliance with Federal laws and regulations. In addition, the policies should address Web page format, standardization, and content; training program for Web presence management; Web security; and operational procedures, such as change and configuration management. Policies should also include other areas such as cost/benefit analysis, E-mail inquiries, E-government initiatives, and hosting or outsourcing Web sites.

MOVING TO A CUSTOMER-CENTERED WEB PRESENCE

FOCUSING ON THE CUSTOMER

- Use the Web presence to focus on the customer by providing enhanced quality and availability of products, services, and opportunities; improved timeliness of information; better accessibility; and improved mission achievement. We suggest that DOI:
 - Identify the products, services, and opportunities that it offers customers, and identify those that could be made available through the Web.
 - Identify DOI customers and determine their wants and expectations.
 - Align or focus products, services, and opportunities toward customers. For example, on DOI's "Collaborative Efforts - Conserving Endangered Species through Partnerships" it informs customers of what the results were of partnership activities instead of how the customer could become a partner in this conservation program.
- Centrally locate access points to the existing products, services, and opportunities that customers want based on the results of the above suggestions. DOI should consider portal technology so that a customer who is not familiar with DOI can easily find specific information without extensive knowledge of DOI or the Web. (See Figure 3 on page 5 for business activities of DOI that can be found throughout DOI's Web presence at multiple access points.)
- Review current Web sites and pages for the characteristics listed below. Based on the results of the review, take action either by correcting the site or page or removing it. The review should determine whether:
 - Information is timely.

- Information is accurate, consistent, and not redundant.
- Web pages are accessible within a reasonable amount of time via any connectivity method.
- Sites are accessible to all customers, to the maximum extent possible, by meeting Section 508 of the Rehabilitation Act Amendments of 1998.
- Privacy policies, including children's privacy, are easily reached on any Web access point.
- Information is not requested and collected from children without parental consent.
- Customers are notified upon departure from DOI sites.
- Persistent cookies are not used without the required approvals. The DOI CIO should disable Web sites that contain persistent cookies until the DOI Web Master is provided assurance that: (1) sites give clear and conspicuous notice of the use of persistent cookies; (2) there is a compelling need to gather the data on the site; (3) appropriate and publicly disclosed privacy safeguards exist for handling any information derived from the cookies; and (4) appropriate bureau or office heads or the Director of DOI's National Business Center have formally approved the use of each persistent cookie.

See Appendix 4 on page 28 for the results of our review of some of these features on selected DOI Web sites.

ESTABLISHING A STRATEGY

Develop an E-government strategic plan to use IT to transform the way DOI works to improve services to its customers. DOI should complete a strategic plan that includes:

- E-government mission and vision that aligns with DOI's Strategic Plan, IT Strategic Plan, and the Interior Enterprise Architecture objectives.
- Applicable legal requirements including security, privacy, and records management.
- Goals and associated objectives supporting the mission and vision.

- Metrics to measure performance for achieving the goals. These metrics should, at a minimum, measure:
 - Use of resources to maintain Web presence.
 - How well the Web sites meet the needs of customers.
 - How much the Web sites are contributing to customers taking advantage of the opportunities offered through DOI's Web presence and enabling DOI to better accomplish its mission.
- Short- and long-term steps and success factors to achieve the desired outcomes.

ENSURING TRANSFORMATION CONTINUES

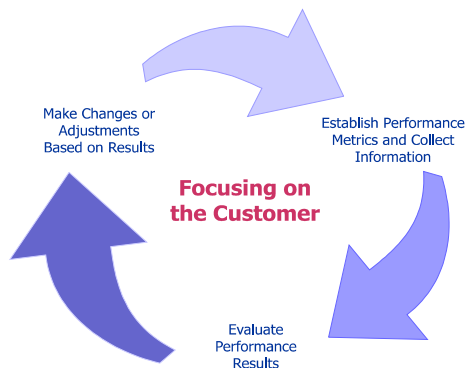


Figure 9. Cycle To Ensure Web Presence Remains Customer Focused.

A best practice contributing to transforming from a bureaucracy-centered to a customer-centered Web presence is developing and implementing a strategy for managing Web content and design to focus on customers' wants. To achieve this transformation, we suggest that DOI develop Web content management and design policies and procedures that include:

- Periodically reassessing what customers want using methodologies such as analyzing: (1) systems logs, for example, to determine the numbers of times and the amounts of time each site is visited or is accessed; (2) key word searches; (3) frequently requested information; and (4) online customer satisfaction surveys.
- Creating a uniform look across DOI to include a standardized Web site design. The design should ensure that when Web sites are accessed the customer is made aware that it is a DOI Web site. While bureau-specific information can be provided, it should not confuse the customer that they are somewhere other than DOI. This can be accomplished by developing templates to standardize the look and feel of DOI Web sites and pages as well as filtering out unwanted content.

- Periodically evaluating the accessibility of the Web sites for broken links, orphan pages, connectivity issues, and user friendliness features, and ensuring deficiencies are corrected.
- Ensuring information that is posted on DOI Web sites is consistent, up-to-date, and not redundant.
- Moving or eliminating unnecessary or unwanted information not of interest to the public customer. Pertinent information for DOI employee users should be placed on a DOI intranet.
- Improving the efficiency of maintaining and posting information and the ability for users to customize the information they want by requiring, to the extent possible, pages to be dynamic (where information is found through queries to a database) rather than static (which is similar to hard-copy information where changes require rewriting the Web page).
- Defining what is sensitive information that should not be posted on the public Web sites.
- Standardizing all Web sites that are designed for children to include requirements for parental consent before information is requested and collected from children under the age of 13 thus complying with the Children's Online Privacy Protection Act.
- Ensuring privacy statements and Freedom of Information Act [5 U.S.C. § 552 as amended by Public Law 104-231, 110 Stat. 3048] procedures are accessible from each Web page and ensuring that disclaimer statements are consistent with the DOI Information Quality Guidelines.
- Ensuring information is grouped around lines of business and services and allowing access through portal technology rather than through multiple sites.

ENHANCING SECURITY

NEAR-TERM

Implement procedures to protect information and servers from loss, misuse, or modification and unauthorized access through minimizing vulnerabilities and mitigating threats to an acceptable level. To enhance the security of its Web sites, DOI should:

- Inventory Internet access points and eliminate or consolidate to reduce the total numbers of Internet access points throughout DOI.
- Document the Internet access points on network topologies, including connections to hosted and outsourced servers.
- Ensure that the required security architecture, which should include DOI Web sites and those sites that are outsourced and hosted, are in a DMZ.
- Develop a naming standard for hosts or network devices to prevent the easy identification of operating systems or functions from the Internet. For example, a device with the name “*doi-firewall-sw*” could easily be identified as a firewall.
- Perform periodic risk assessments on Internet access points and implement appropriate controls to protect internal networks.
- Perform risk assessments and privacy impact assessments prior to deployment of new Web sites.
- Ensure Web server software and related operating systems are updated with the most recent patches or fixes. (See Figure 4 on page 8 for current versions available of Web server software and examples of what is used on DOI Web servers.)
- Establish configuration standards for DOI Web architecture and develop configuration management policies and procedures.

KEEPING DOI’S Web PRESENCE SECURE

- Consolidate, physically and logically, DOI and bureau Web servers to the maximum extent possible.
- Ensure DOI's Web presence is addressed in security plans and is incorporated into the Certification and Accreditation process for DOI's networks.

Using our framework, DOI should be able improve its Web presence by focusing on the customer, enhancing security, maintaining privacy, reducing duplication, and, in the long term lowering costs.

RECOMMENDATION

We recommend that the DOI CIO develop and implement a plan, based on the framework identified in this report, for centrally controlling and managing DOI's Web presence.

EVALUATION SCOPE AND METHODOLOGY

SCOPE OF EVALUATION

Our evaluation included all the Department of the Interior's (DOI) and its components' (bureaus and offices) Web sites and pages that were available for access by the public and were connected to the Internet during November 2002 through March 2003. Web sites that were not available and therefore not included in our evaluation were those of the Bureau of Indian Affairs, the Office of Hearing and Appeals, and the Office of Special Trustee for American Indians. In addition, we limited our review of the Office of Indian Education .edu Web sites to determining the numbers of domains and Web sites. Office of Indian Education .edu Web sites were not subjected to Web presence analysis because they serve a different function than the other DOI sites. Finally, we limited our review to only http:// and https:// which are the basic means for customers to interact with the World Wide Web and to download requested information.

We reviewed DOI and its components' policies and procedures related to managing and controlling Web sites. We also interviewed DOI personnel responsible for maintaining Web sites and servers. We evaluated DOI processes and its publicly available Web sites and compared these to best practices that we developed from our reviews of various Federal and state agencies Web sites; Federal agencies' Web procedures and practices; and Office of Management and Budget, National Institute of Standards and Technology, and industry standards.

We performed this evaluation in accordance with the "Government Auditing Standards" issued by the Comptroller General of the United States. Accordingly, we included tests and other procedures that were considered necessary under the circumstances.

WEB DOMAINS AND SERVER REVIEW

To identify DOI's domains and Web servers and to determine whether security was adequate, we used several network surveying software tools to identify and analyze DOI's and its components' domains, Web sites, servers, and networks.

We used Web crawler software programs to identify DOI's Web domains and sites and Web site configurations. We also used these tools to identify Web sites hosted by DOI that may be unauthorized and DOI Web sites that were hosted outside of DOI. From this information, we identified DOI's IP addresses related to DOI's Web presence. In addition, we used a network-mapping tool to identify hosts that were not identified by the Web crawler tool. This tool also provided us with lists of hosts, servers, and other network devices such as routers, switches, firewalls, and printers that were identifiable from the Internet.

WEB SITE REVIEW METHODOLOGY

We developed a checklist based on identified best practices for Web site content and features (see Appendix 4 on page 28 for results of our evaluation). We evaluated these features on the following selected 70 Web sites:

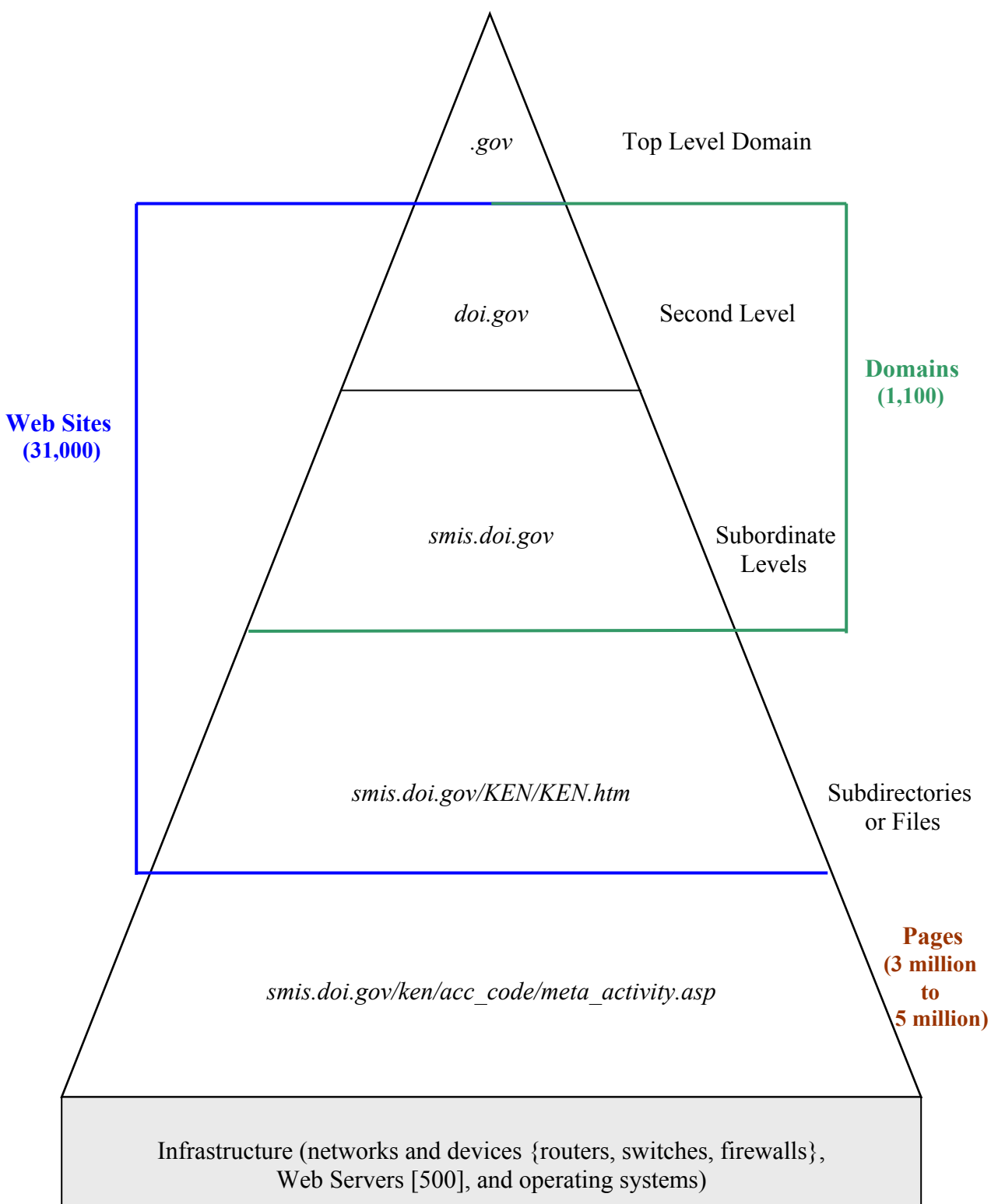
- 56 tab pointer links from the eight tabs listed on *www.doi.gov* – Collaborative Efforts, American Indians, Fish/Wildlife, National Parks, Public Lands, Energy, Science, and Water
- 9 bureau and DOI home pages
- 5 judgmentally selected DOI and bureau Web sites

WEB SITES REVIEWED

Bureau	Number of Sites Reviewed
U.S. Geological Survey (USGS)	23
National Park Service (NPS)	9
Bureau of Land Management (BLM)	8
Minerals Management Service (MMS)	8
U.S. Fish and Wildlife Service (FWS)	7
Department of the Interior (DOI)	7
Bureau of Reclamation (BOR or USBR)	5
BLM and Forest Service	1
National Business Center (NBC)	1
Office of Surface Mining Reclamation and Enforcement (OSM)	1
Total	70

In addition to the 70 sites, we judgmentally selected numerous other DOI Web sites and pages. We reviewed these Web sites and pages for features, such as redundant, duplicated, sensitive, and inconsistent information; ease in accessing information; compliance with Federal laws and regulations; hosting other organizations' Web sites; and Web content and site design. Further, we evaluated business cases for selected DOI Web sites, if business cases were developed, and contracts and costs for DOI Web sites hosted on third-party Web servers.

DIAGRAM OF THE DEPARTMENT OF THE INTERIOR'S WEB PRESENCE







DEPARTMENT OF THE INTERIOR'S “OTHER” WEB SITES

The Department of the Interior’s (DOI) Web presence includes approximately 1,100 domains (addresses). Of these addresses, 15 percent do not include the “DOI” or bureau, such as “BLM,” “NPS,” or “USBR,” acronyms as shown in Figure 1 on page 1 of the report. Examples of the “Other” Web sites follow:

























































americasoutdoors.gov	handsontheland.gov	partnersinflight.org
anaskforce.gov	historicpreservation.gov	pbin.nbii.gov
baca.gov	icbemp.gov	permits.gov
bacaranch.gov	industrialecology.gov	piedrasblancas.gov
bianifc.org	infms.gov	pnwin.nbii.gov
bioeco.gov	interior.gov	recreation.gov
birdcon.nbii.gov	invasivespecies.gov	redondopeak.gov
cain.nbii.gov	invasivespecies.nbii.gov	reo.gov
cal-parks.ca.gov	lacoast.gov	safenet.nifc.gov
cesu.org	landfire.gov	safety.oas.gov
cleanwater.gov	lewisandclark200.gov	sain.nbii.gov
clear.search.gov	liss.org	science.gov
clearinghouse1.fgdc.gov	mbr.nbs.gov	sciencerule.gov
clearinghouse2.fgdc.gov	mesc.nbs.gov	seagrannews.org
clearinghouse3.fgdc.gov	metadata.nbii.gov	search.nbii.gov
clearinghouse4.fgdc.gov	mrlc.gov	senrlg.gov
cswgcin.nbii.gov	msc.nbs.gov	sierranewadawild.gov
ec21.gov	nationalatlas.gov	sierrawildbear.gov
ein.nbii.gov	nbii.gov	snow.water.ca.gov
emtc.nbs.gov	nbs.gov	swin.nbii.gov
eric.ed.gov	ndep.gov	urban.nbii.gov
far.nbii.gov	nemi.gov	usfilm.gov
fgdc.gov	nepa.gov	usitc.gov
firejobs.gov	nfpors.gov	usparkpolicenyfo.gov
fireleadership.gov	nifc.gov	vallegrande.gov
frogweb.gov	nifc.org	vallesgrandenationalpreserve.gov
gai.fgdc.gov	nigc.gov	vcnp.gov
gapanalysis.gov	nrin.nbii.gov	volunteer.gov
gcmrc.gov	nrtc.gov	westnilevirus.nbii.gov
genetics.nbii.gov	nwcg.gov	wildlandfire.gov
geocommunicator.gov	nwfireplan.gov	wildlandfires.gov
geomac.gov	oas.gov	wildlifedisease.nbii.gov
geo-one-stop.gov	oregontrail.gov	windowsintowonderland.org
govworks.gov	osti.gov	yourland.gov

SCORECARD OF THE DEPARTMENT OF THE INTERIOR'S WEB SITES

We developed a rating system to evaluate specific features on Department of the Interior's (DOI) Web sites. Our ratings were determined from information collected from 70 DOI Web sites based on Office of Inspector General (OIG)-developed checklists containing specific best practices attributes. If the Web site had a specific attribute, it received a score of 5 and if it did not have the attribute it received a 0. Answers, such as "possibly," "somewhat," or "limited," received a score of 2.5. In addition to determining a rating score for each attribute, we developed a color-coded system to better depict the areas that were adequate, in need of improvement, or inadequate. The following table provides the color code, the corresponding rating interval, and description.

		Rating Score	Description
COLOR KEY		0-2.0	Inadequate
		2.01-3.75	In Need of Improvement
		3.76-5	Adequate
			Not Applicable

The following table is a summary of the results of our evaluation of DOI's Web sites by an OIG-determined sample group: DOI Tab Pointer Links found on DOI's home page, DOI and bureau home pages, and other judgmentally selected sites. The features we evaluated were categorized by User Help Features, Service Navigation Features, and Other User Friendly Attributes.

	<i>DOI Tab Pointer Links</i>	<i>Home Pages</i>	<i>Other Sites</i>	<i>Overall Score</i>
User Help Features				
1. Comments and Feedback				
2. Search				
3. Index				
4. Site Map				
5. About the Site				
6. Frequently Asked Questions (FAQ)				
7. Help				
Overall Ranking for User Help Features				
Service Navigation Features				
8. Welcome				
9. Just For Kids				
10. Maps				
11. In the Newsroom/In the News				
12. Freedom of Information Act (FOIA)				
13. Events				

	<i>DOI Tab Pointer Links</i>	<i>Home Pages</i>	<i>Other Sites</i>	<i>Overall Score</i>
14. What's New				
15. About Services				
16. Links to Other Agencies/Regions				
<i>Overall Ranking for Service Navigation Features</i>				
Other User Friendly Attributes				
17. Page does not link to intranet log-in				
18. Duplicate information not found on pages tested				
19. Information was current or not expired				
20. Contact information - Phone number and addresses available				
21. Obvious link to contact information				
22. No personally sensitive information on page				
23. Link to Privacy Policy statement				
24. External links with proper exit notices				
25. No persistent cookies				
26. Link to Disclaimer statement				
27. Site compliant Section 508 of the Rehabilitation Act				
28. Page links to next hierarchy (within Bureau)				
29. Home page has link to DOI				
30. Customers can E-mail the Webmaster				
31. Customers can E-mail the Pagemaster				
32. Customers can E-mail other individuals				
33. Foreign language access				
34. Easy to use and accessible				

GLOSSARY OF TERMS USED

A-D

COOKIE

A message given to a Web browser by a Web server. The browser stores the message in a text file on the users' computers. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly prepare customized Web pages for them. Generally, there are two types of cookies, session and persistent. The session cookie exists only when the user is browsing the Internet. The persistent cookie exists during the time the user is browsing the Internet as well as after the user closes the browser.

DMZ

A Demilitarized Zone is a network configuration used to provide security while allowing Internet traffic to access services such as a Web site (http), file transport protocol (FTP) servers, electronic mail (E-mail), and Domain Name Servers (DNS). The DMZ is the first line of defense between the Internet and an organization's internal networks and is usually a combination of firewalls and other computer hardware or software devices.

DOMAIN

A domain is a set of network addresses that is organized in levels. The top level identifies purpose commonality (for example, the organization that the domain covers such as ".gov"). The second level identifies a unique place within the top level domain and is equivalent to a unique address (such as "doi.gov") on the Internet. Lower levels on the domain may also be used (such as "smis.doi.gov").

E-H

FIXES – SEE PATCHES

HOST

A computer that is attached to a computer communications network that can use services provided by the network to exchange data with other attached computers and networks.

HTTP

Hypertext Transfer Protocol is the standard Internet Protocol for the exchange of information using World Wide Web (Web) technology.

HTTPS

An extension of the *Hypertext Transfer Protocol* that is designed to transmit individual messages securely.

I-L

INTERNET

The Internet is a network of networks. It is a system of linked computer networks, international in scope, that facilitates data transfer and communication services, such as remote login, file transfer (FTP), electronic mail (E-mail), newsgroups, and the World Wide Web.

INTERNET ACCESS GATEWAYS OR POINTS

A network device interface that connects the internal network and the Internet to provide users connected to the internal private network access to the Internet. It allows traffic both ways and it is usually referred to as a gateway.

IP ADDRESS

Is the abbreviation for Internet Protocol address commonly referred to as an IP. It is a numeric address that is given to servers and hosts connected to the Internet. For servers, it is translated into a domain name by a Domain Name Server (DNS). For hosts, it is assigned by the Internet Service Provider (ISP).

M-P

NETWORK DEVICE

Any machine or component that attaches to a communications network. Examples of network devices include servers, firewalls, routers, switches, hubs, bridges, and modems.

ORPHAN PAGE

The name for a Web page that has been abandoned but still remains available.

PATCH

A supplemental software code that, when installed to the original software program, fixes problems (bug). A patch can usually be downloaded off the Internet in order to fix a software problem or security vulnerability.

PORTAL TECHNOLOGY

A technology strategy for facilitating the dissemination of information, providing self-service capabilities, and improving communications and interaction with and in between customers.

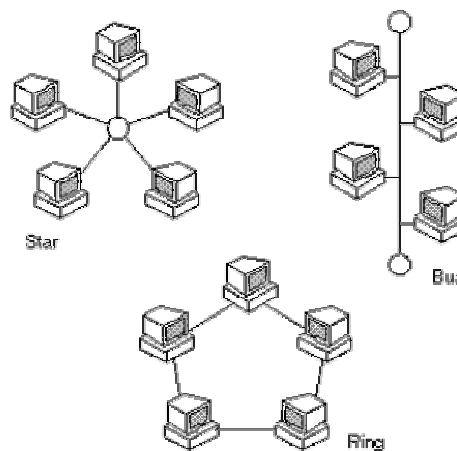
Q-T

THREAT

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability. A threat can be either "intentional" (for example, an individual cracker or a criminal organization) or "accidental" (for example, the possibility of a computer malfunctioning or natural disaster such as an earthquake, a fire, or a tornado).

TOPOLOGY

The shape of a local-area network (LAN) or other communications system network. Topologies are either physical or logical. Three basic topologies are shown below:



U-Z

URL

Abbreviation of *Uniform Resource Locator*, it is the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, for example *http*, and the second part specifies the IP address or the domain name where the resource is located.

For example, the two URLs below point to two different files at the domain *usbr.gov*. The first specifies an executable file that should be fetched using the File Transfer Protocol; the second specifies a Web page that should be fetched using the Hypertext Transfer Protocol:

`ftp://ftp.usbr.gov/stuff.doc`
`http://www.usbr.gov/main/index.html`

VULNERABILITY

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system configured security policy.

WEB CRAWLER (ALSO KNOWN AS WEB SPIDER)

A program that automatically fetches Web pages. Crawlers or spiders are used to feed pages to search engines. Because most Web pages contain links to other pages, a crawler can start almost anywhere. As soon as the crawler sees a link to another page, it goes off and fetches that page. Large search engines, like Alta Vista, have many crawlers working in parallel.

WEB PAGE

A document on the World Wide Web. Every Web page is identified by a unique URL.

WEB PRESENCE

An organizations' established World Wide Web existence, through Web sites or a collection of Web files. It includes all components needed to provide the information published or posted on Web sites to be accessed or used by customers.

WEB SERVER

A Web server or Internet server is a computer that stores files of various types and makes them available over the Internet. A Web server stores the Web pages and provides them to users using Web "browser" software via the Internet.

WEB SITE

A location on the World Wide Web. Each Web site contains a home page, which is the first document users see when they enter the site. The site might also contain additional documents and files that may also be considered Web sites. A site can be owned and managed by an individual, company, or organization. This term is frequently used to identify anything located on the World Wide Web including a Web domain or a Web page within a domain.

WORLD WIDE WEB

A hypertext-based system for finding and accessing Internet-based data and information resources. It is capable of providing the public with user-friendly graphics-based access to information on the Internet. It is the most popular means for storing and linking Internet-based information.

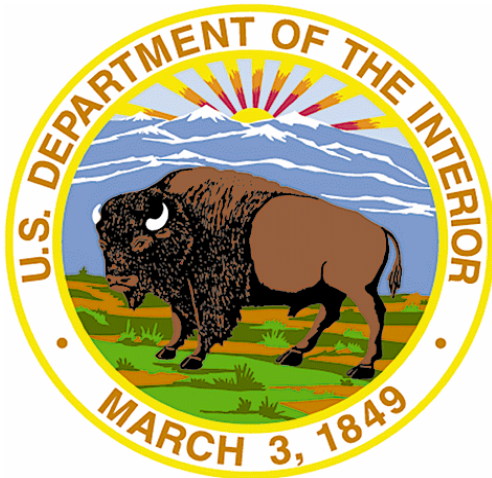
How to Report Fraud, Waste, Abuse and Mismanagement

Fraud, waste, and abuse in government are the concern of everyone – Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and abuse related to Departmental or Insular Area programs and operations. You can report allegations to us by:

Mail: U.S. Department of the Interior
Office of Inspector General
Mail Stop 5341-MIB
1849 C Street, NW
Washington, DC 20240

Phone: 24-Hour Toll Free 800-424-5081
Washington Metro Area 202-208-5300
Hearing Impaired (TTY) 202-208-2420
Fax 202-208-6081

Internet: www.oig.doi.gov/hotline_form.html



U.S. Department of the Interior
Office of Inspector General
1849 C Street, NW
Washington, DC 20240

www.doi.gov
www.oig.doi.gov