

**Audit of the Controls over Inappropriate Personal Use of the
Internet at NARA**

OIG Audit Report No. 11-10

March 8, 2011

Table of Contents

Executive Summary.....	3
Background.....	4
Objectives, Scope, Methodology.....	5
Audit Results.....	6
Appendix A – Example of [REDACTED] Accessed with no Web Filter Restriction.....	16
Appendix B – Example of Web Filter Bypass [REDACTED].....	17
Appendix C – Example of a Site Accessed by [REDACTED] [REDACTED].....	18
Appendix D – Example of Inappropriate Sites Accessible through Message Boards and Forums.....	19
Appendix E – Example of Discrepancies in Sites Blocked across NARA's Network.....	20
Appendix F – Management's Response to the Report.....	21
Appendix G – Report Distribution List.....	22

Executive Summary

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) completed an audit of NARA's controls over the inappropriate personal use of the internet by NARA staff. NARA has established policy over the staff's usage of the internet, which the Office of Information Services (NH) and the Office of Administration (NA), with the support of General Council (NGC), monitor and enforce. During this audit, we assessed the effectiveness of the controls and procedures NARA has in place to fully implement its policy.

In May 2010, NARA issued revised Directive 802, *Appropriate Use of NARA Office and Information Technology (IT) Equipment and Resources*, authorizing staff to use NARA office and IT equipment and resources when performing limited personal use during non-work time, provided the use does not interfere with official business or involve inappropriate use. Within the scope of this audit, the Directive defines inappropriate personal use as that in which a NARA employee engages in activities that are illegal or offensive. This includes accessing materials that are sexually explicit or involve gambling, weapons, or terrorist activities. In the past, NARA relied almost exclusively on its automated web filtering application to ensure NARA staff were not accessing inappropriate material. However, due to the failures of similar controls at other agencies recently coming to the attention of Congress and the media, NARA supplemented its web filtering application with monthly reporting procedures.

Our review found that although NARA has invested in tools and implemented procedures to monitor and prevent inappropriate internet usage by its staff, controls remain inadequate and NARA employees continue to access prohibited material. NARA staff have been able to bypass the web filter and go undetected for the past four years, as this is when NARA began relying almost solely on its web filtering application to automatically block inappropriate use. NARA's web filtering application is generally successful in blocking the majority of NARA staff that carelessly or inadvertently attempt to access inappropriate material. However, as reported at other agencies, the real risk comes from the staff who regularly bypass the inappropriate use controls, which was not found to be difficult at NARA. NARA's web filtering application maintains a record of all NARA staff internet usage—which is invaluable in detecting employees who bypass the controls—however, even after NARA recently implemented its monthly reporting process, the limited amount of information reviewed and analysis conducted by NARA allowed excessive personal and inappropriate use to go undetected or unaddressed. Consequently, NARA is at risk for decreased public trust, reduced employee productivity, legal liability, and degradation of network performance.

Our audit identified several improvements to be made to NARA's controls in preventing its staff from inappropriate use of computer resources. We made five recommendations to more thoroughly ensure that NARA Directive 802 is enforced and risks are minimized.

Background

NARA continues to embrace the ever increasing efficiencies of the internet in performing its mission. Examples are contained throughout the FY 2010 Performance and Accountability Report, which includes NARA's ongoing efforts to utilize social media and internet networking tools as a way to communicate and deliver timely information to the public. Furthermore, NARA—like nearly all modern organizations—depends on the internet at the most basic level for its employees to perform research, stay informed with current events affecting their job responsibilities, and communicate with fellow colleagues and NARA business partners.

In addition to internet usage by staff in support of NARA's mission, NARA also recognizes the benefits of allowing staff to access the internet for limited personal use while at work. NARA Directive 802, *Appropriate Use of NARA Office and Information Technology (IT) Equipment and Resources*, specifically allows this in an effort to create a more supportive work environment. Benefits of such a policy generally go undisputed. However, left unchecked, some employees will inevitably abuse such privileges putting the agency at risk.

An example of employee abuse of the internet within another federal agency was reported in the media this past year. Ongoing investigations at the Securities and Exchange Commission (SEC) discovered a number of SEC employees were attempting to access inappropriate material on the internet while at work. One of the SEC investigations was conducted at the request of a U.S. Senator. The investigations discovered the SEC's web filter blocked many of the attempts made by its staff, however, employees were able to bypass the filter and gain access to a significant number of inappropriate sites.

Shortly after the most recent SEC investigation was reported, NARA began developing a procedure to supplement the web filter control that had been in place since 2007. This procedure involved the Office of Information Services (NH) using the web filter application to generate reports listing NARA staff with multiple blocked website access attempts in the categories defined as inappropriate by NARA Directive 802. The initial report was run for a one week period at the end of April 2010, at which time it was provided to the Office of Administration (NA) and General Council (NGC). The report indicated ongoing abuse had been taking place, for example, one NARA employee identified in the report accumulated 40,000 blocked attempts during the initial one week reporting period. Beginning in July 2010, NA and NGC began receiving this report on a monthly basis.

Inappropriate internet usage by NARA staff is not a new occurrence at the Agency. The OIG previously reported on this matter in April 2003. Following the 2003 review, NARA developed corrective actions that were initially put in place to monitor and deter inappropriate internet usage in accordance with NARA Directive 802. However, as the controls in place continue to evolve, NARA must ensure the associated risks remain mitigated.

Objectives, Scope, Methodology

The overall objective of this audit was to determine whether NARA's controls were adequate and effective in preventing and deterring NARA staff from using their government-assigned workstations to access inappropriate internet material, as defined by NARA Directive 802, *Appropriate Use of NARA Office and Information Technology (IT) Equipment and Resources*. Our review focused on whether NARA employees were in compliance with directives restricting access to inappropriate web sites, and whether controls and administrative processes in place adequately prevent and deter NARA staff from accessing these sites.

To accomplish our objective, we interviewed key NARA personnel and contractor staff from the Office of Information Services and the Office of Administration and examined NARA policies governing the appropriate use of the internet. We gained an understanding of NARA's internet monitoring process, web filtering application, and administrative and disciplinary procedures. We obtained the monthly agency-wide reports listing NARA staff with multiple blocked website access attempts and from these reports, judgmentally selected samples of specific NARA staff with high numbers of blocked attempts. For the NARA staff sampled, we requested detailed internet usage logs, which were generated using NARA's web filtering application. The monthly reports and detailed user logs were analyzed extensively by the auditors to determine the methods and degree of inappropriate usage and the effectiveness of the procedures in place to prevent such activity. The usage logs only contained data from when the users were connected to NARA's network, therefore, usage data while working from home with a personal internet connection was not included in our review.

Our audit work was performed at Archives II in College Park, MD between September 2010 and January 2011. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results

Controls to Prevent NARA Staff from Accessing Inappropriate Material are not Fully Effective

Although NARA has invested in tools and implemented procedures to monitor and prevent inappropriate internet usage by its staff, NARA employees continue to access prohibited material. This condition exists because NARA is over confident in the effectiveness of its web filtering application, does not fully utilize the features of this application, and has not established adequate procedures to consistently enforce its policy on inappropriate internet usage. As a result, NARA is at risk for decreased public trust, reduced employee productivity, legal liability, and degradation of network performance.

In May 2010, NARA issued revised Directive 802, *Appropriate Use of NARA Office and Information Technology (IT) Equipment and Resources*, maintaining authorization for NARA staff to use NARA office and IT equipment and resources when performing limited personal use during non-work time so long as the use does not interfere with official business or involve inappropriate use. The Directive provides examples of inappropriate use, which (within the scope of this audit) include:

- Using NARA office equipment to engage in activities that are illegal or offensive to fellow staff or the public,
- Creating, downloading, viewing, storing, copying, or transmitting sexually explicit or sexually oriented materials,
- Engaging in any activity prohibited by law or regulation, including illegal gambling, weapons, or terrorist activities,
- Any use of NARA office equipment that could generate more than minimal additional expense to NARA, and
- Downloading games and/or playing them during official business hours.

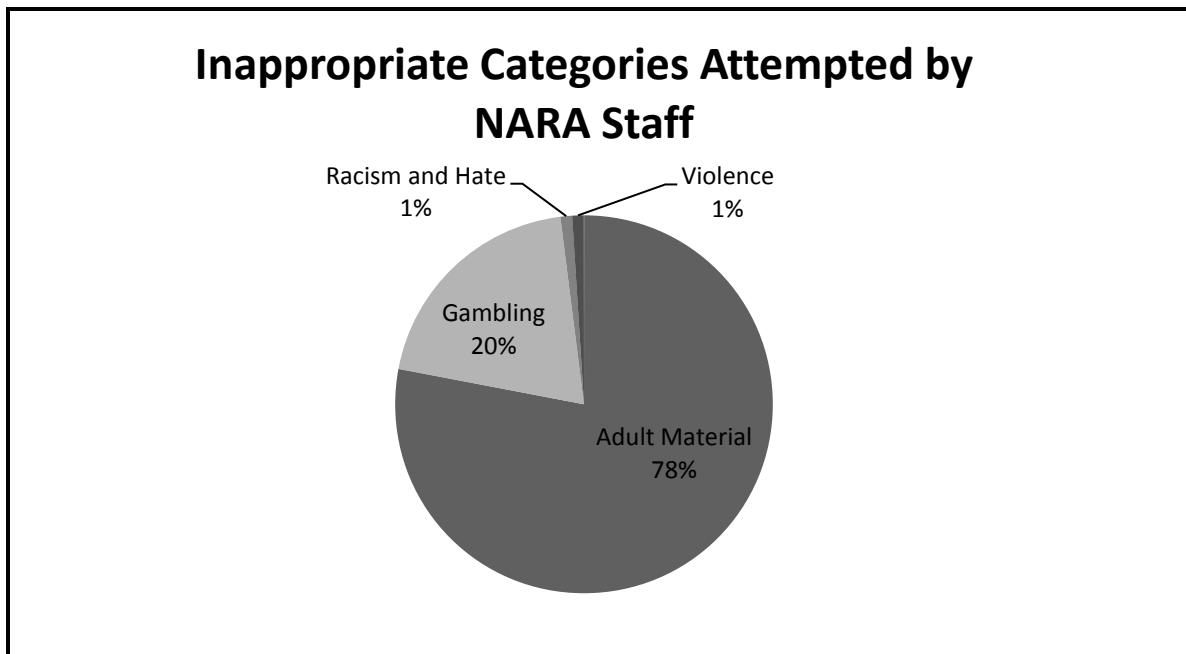
The Directive stipulates NARA has the right to block access to sites that may contain inappropriate content. Further, the Directive states NARANET system managers use monitoring tools to detect improper use of the system and IT equipment. Lastly, the Directive identifies the potential consequences of inappropriate use, stating violators may be subject to disciplinary action or prosecution.

During the audited time period, consisting of user data from June 2010 through October 2010, roughly 39% of NARA workstation users made multiple attempts at accessing one or more categories of inappropriate sites monitored by NH, NA, and NGC. These categories include:

- Adult Material: Adult Content,
- Adult Material: Lingerie and Swimsuit,
- Adult Material: Nudity,

- Adult Material: Sex,
- Gambling,
- Racism and Hate, and
- Violence.

Although the numbers are alarming, attempts at accessing sites falling within these categories can at times be made unintentionally by NARA staff during normal internet usage. However, the information above is calculated using the threshold—five or more attempts per category, per month—established by NH, NA, and NGC in their monthly reporting and monitoring practices. The majority of attempted inappropriate internet site visits made by NARA staff fell into the “Adult Material” categories, the proportions are presented in the chart below.



Of the NARA staff who attempted to access inappropriate sites, on average, 90% made fewer than 50 attempts in each of the months analyzed. The remaining 10% of NARA staff listed in the monthly reports individually attempted to access inappropriate sites from 50 to as high as 13,816 times during the months analyzed. In certain situations, high attempts at accessing inappropriate material can be a result of users inadvertently loading malware onto their NARA workstations. However, the analysis performed on the individual user logs of the staff sampled for this review indicated the users intentionally attempted to access inappropriate material on multiple occasions.

Over Confident in the Effectiveness of Web Filtering Application

NH personnel expressed in multiple meetings and correspondence that the current web filter in use, Websense, is more advanced and “robust” than the application NARA used in the past. Therefore, once Websense was implemented in the 2007 timeframe, NH discontinued generating monthly reports detailing inappropriate usage. NH personnel questioned the value of a report showing blocked attempts, as the users theoretically never gained access to the inappropriate sites. However, following more recent discussions with the Archivist regarding

the inappropriate usage at the Securities and Exchange Commission (SEC), NH developed a new monthly inappropriate usage reporting process, which they fully implemented in the July 2010 timeframe.

Prior to the implementation of the new monthly reporting process, NARA relied almost exclusively on Websense to prevent NARA staff from accessing inappropriate websites. Once the new procedure went into effect, NA and NGC began receiving a list of users who had five or more blocked attempts in one or more categories during the month. The reports listed numerous NARA employees who consistently made hundreds and even thousands of attempts to access inappropriate material during each month. Although NA prepared to take disciplinary action against one NARA employee for extensive inappropriate use, the employee left the agency before such actions were executed. Apart from that incident, no other official disciplinary action related to inappropriate usage has taken place since NH initiated the reporting process.

During our review, we selected a sample of users from the monthly inappropriate usage reports NH provided NA and NGC. For the users sampled, we requested the full user internet activity logs (which Websense maintains for every NARA user/workstation for roughly three months). Based on previous correspondence with NH personnel, we expected little evidence of users bypassing the “robust” web filter. However, an initial review of the detailed user activity logs indicated this was not the case. After analyzing the logs more thoroughly, and testing Websense’s capabilities, we identified the following web filter weaknesses:

- NARA staff are able to easily access sexually explicit material [REDACTED]. A few examples of the hundreds of sites visited by NARA staff with no web filter restrictions include “[REDACTED]” and “[REDACTED]”. These sites and others like them contain page after page of sexually graphic images, yet they are categorized by Websense as [REDACTED] which is not a blocked category. One NARA staff member viewed sexually explicit [REDACTED] nearly 4.5 hours in one day, and accessed to some degree 1,300 explicit [REDACTED] in 28 days, with no web filtering restrictions. (See Appendix A for further detail on how NARA staff bypass Websense using this method).
- Users are able to access [REDACTED] designed to bypass Websense and other web filters. By accessing [REDACTED] the user simply [REDACTED]. Websense only recognizes [REDACTED], not the inappropriate site visited [REDACTED]. Websense tracks the user going to [REDACTED] but this information is not included in the monthly reports to NA and NGC. By not following-up on users visiting sites such as “[REDACTED]”, “[REDACTED]”, and “[REDACTED]” NARA is turning a blind eye to users easily bypassing Websense. One user alone accessed [REDACTED] sites 513,537 times over a three

month period. (See Appendix B for further detail on how NARA staff bypass Websense using this method).

- Users [REDACTED] to access inappropriate sites, which likely resulted in the users gaining access. We tested Websense’s blocking ability on a number of the inappropriate sites that were attempted by NARA staff. For the vast majority of sites tested, [REDACTED] would result in successful access (usually only requiring [REDACTED]). Furthermore, even if [REDACTED] of the inappropriate site was blocked by Websense, [REDACTED] containing inappropriate material were often not filtered and easily accessible. On a monthly basis, one user made hundreds [REDACTED] [REDACTED] a website that identifies itself as the “world’s largest sports betting community.” Another user [REDACTED] a website that calls itself the “home of porn,” which contains sexually explicit images and videos. Based on our testing, it is highly likely these users gained access [REDACTED] [REDACTED] (See Appendix C for further detail on how NARA staff bypass Websense using this method).
- Users are able to easily access forums, auction sites, and dating sites for multiple hours per day. Although there may be legitimate reasons for accessing craigslist discussion forums, one NARA staff’s detailed internet activity log showed, for 10 days analyzed, evidence of an average of 2 hours a day devoted to non-work related auctions and forums, some involving dating and sexually explicit topics. The same user was able to frequently access [REDACTED] which identifies itself as “a list of official (listed) and unofficial (hidden/secret/unlisted/ unsupported/homesteaded) craigslist forums.” This directory contains a number of graphic adult forums, which include images and discussions of an inappropriate nature, which are rarely blocked by Websense. (See Appendix D for further detail on how NARA staff bypass Websense using this method).
- Users at [REDACTED] (and possibly other NARA field locations) are not blocked when attempting access to inappropriate websites in uniformity with Archives II. While performing a separate review at [REDACTED] we observed broad access to inappropriate sites while using NARA’s network at this location. In one example, a hack site “[REDACTED]” was accessed with no restriction at [REDACTED] however, the same website was appropriately blocked at Archives II. (See Appendix E for further detail).

Aside from the weaknesses identified above, Websense has intermittent failures that allow NARA staff to access inappropriate sites without restriction. We observed one of these intermittent failures while testing Websense’s capabilities, which lasted nearly 6 hours. NH indicated that they typically do not become aware of intermittent Websense failures except in the rare event in which a NARA user reports the failure. NH explained that they have a known issue with the hardware supporting Websense. If the application becomes saturated

with internet traffic, it may intermittently let inappropriate access requests go through. NARA is in the process of upgrading Websense to a newer version due in part to the current version not always being able to handle NARA staff's internet traffic.

During the entrance conference of this audit, after discussing the SEC's findings of inappropriate use within their agency, an NH official mentioned that the SEC's situation was likely a result of not having anyone monitor or look at the records. In a follow-on meeting, another NH official stated that the SEC did not have a web filtering product "as good as Websense." However, until recently, NARA had not been looking at its own staff's inappropriate usage records, but instead relied almost exclusively on its web filtering application to prevent access to prohibited sites. As confident as NARA may be in its perceived "robust" web filtering application, NARA staff are easily able to bypass Websense. This was clearly evident by the sample of user logs analyzed during our review. Once informed of the methods NARA staff used to bypass the web filter, NH agreed that the sites accessed should have been blocked by NARA's web filter and that the current control procedures are not identifying all inappropriate user activity. Further, NH agreed the information pertaining to the bypass methods identified in this report should be used in developing revised control reporting methods in conjunction with NA and NGC.

Underutilization of Available Web Filtering Application Features

NARA is in the process of upgrading to a newer version of Websense. The most recent one year renewal of Websense licenses and support amounted to just over \$158,500 (this figure does not include the associated hardware upgrades). However, even with the older version, NARA was not using all the Websense features available to deter and monitor NARA staff's inappropriate use of the internet. The following Websense functions are underutilized by NARA:

- Reporting. Websense allows the administrator to generate standard and customizable reports on all user information (going back as far as approximately three months). See Figure 1 below for a screenshot of Websense's standard report menu. Examples of the standard Websense reports include: "which users were blocked most," "top users in adult categories," and "users that spent the most time on [non-] productivity sites." In addition to the many useful standard reports, NH can also generate customized reports pulling whatever data is needed, either by groups or individuals, real-time or historical timeframes, for any or all categories. Once NH establishes the customized report criteria, as with the standard reports, one click of the mouse begins the automatic process of pulling the data. Currently, NA and NGC only receive a summary report of the blocked attempts for the seven categories defined earlier. User detail reports could also be generated for a specific number of top blocked NARA staff in each category, which would provide NA and NGC more information in deciding whether to pursue disciplinary actions. In addition, NH could generate web proxy reports to determine the extent of NARA staff bypassing the web filter [REDACTED]

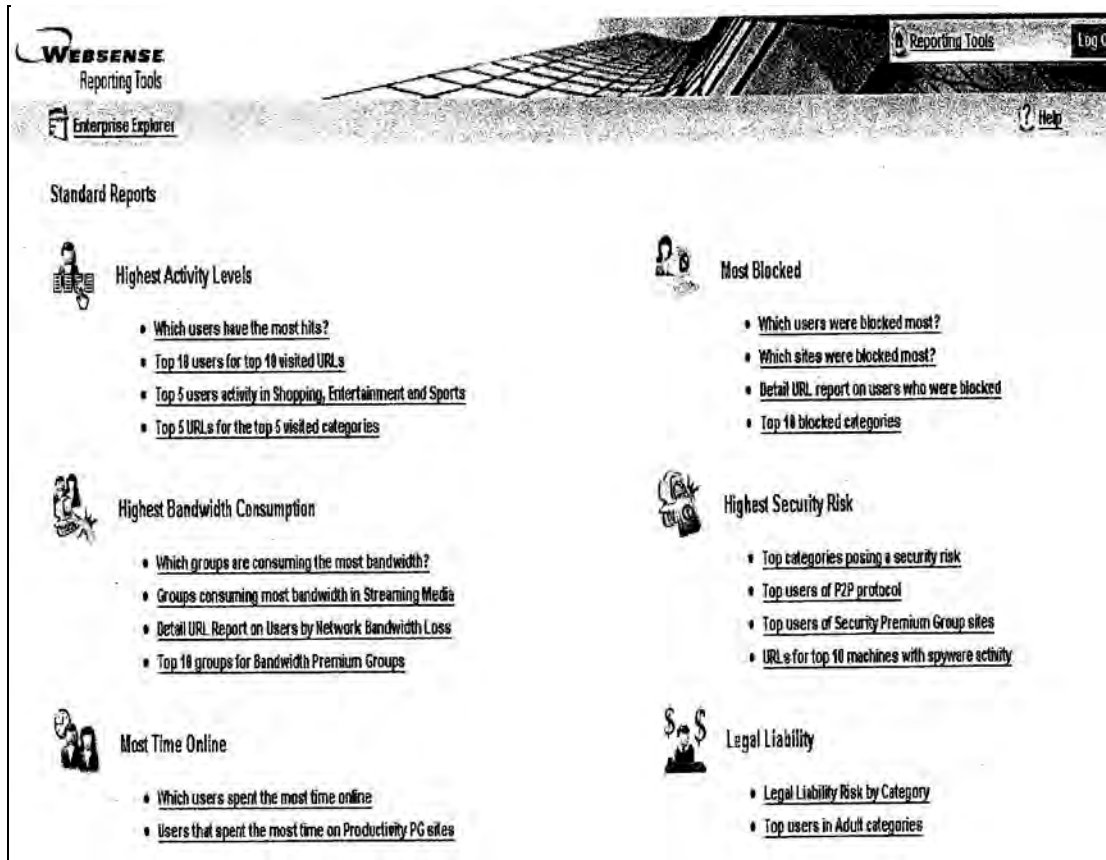


Figure 1. Screenshot of Websense Standard Reports

- **Real-Time Alerts.** Websense allows the administrator to set up alerts based on a multitude of factors. For example, an e-mail alert could be sent to NH whenever a NARA employee surpasses 100 blocked “Adult Material: Sex” sites during a 24 hour period. NH could provide this timely information to NA for further action. Currently, NH only uses this form of Websense alerts in the context of network performance; however, this function would also be useful in monitoring inappropriate internet usage and enforcing NARA Directive 802.
- **Keyword Blocks.** Websense allows the administrator to establish filtering restrictions that block sites whose web addresses (URLs) contain certain words. When keyword blocking is activated for a category, Websense software blocks any site whose URL contains a keyword assigned to the category. For example, NH could review the user activity of NARA staff that access inappropriate [REDACTED] (as discussed previously) and select keywords to block that are obviously inappropriate.
- **Limit by Quota.** Websense allows the administrator to establish user, group, workstation, or network time quotas for defined categories. During this review, while observing the Websense application in use by an NH contractor, a real-time report showed that Facebook was the most active website at NARA. Based on that

information, an example of the quota function would be for the administrator to set an arbitrary 2 hour maximum time quota for the category “Society and Lifestyles [Social Networking],” which would prevent defined groups of NARA staff from accessing Facebook for more than 2 hours each day.

- **Time Period Policy.** Similar to the time quota feature, Websense allows the administrator to define policies for NARA staff’s access to specific categories at certain times of the workday. For example, NH could set Websense to allow access to sites that tend to be personal (i.e., internet auctions, real estate, dating, etc.) only during the hours surrounding lunchtime.

NARA has already invested in the Websense application and these features are available for NARA’s use, however, NH has not implemented all the Websense tools available to effectively enforce NARA Directive 802. Consequently, NARA underutilizes features that assist in blocking access to inappropriate websites and enhance NARANET system managers’ capabilities in meeting their responsibilities in monitoring and detecting improper use of NARA’s system and IT equipment. NH indicated it is not their responsibility to determine what Websense features are put to use, however, NH agreed NARA management should be informed of these features in order to decide whether they should be implemented.

Lack of Enforcement of NARA 802

The effectiveness of NARA Directive 802—like all policy—is in large part dependent upon the degree to which it is enforced. NARA 802 states NARANET system managers use monitoring tools to detect improper use of the system and IT equipment. However, in meetings with NH and NA officials, it became apparent the responsibilities of monitoring are not well defined. NH officials indicated NA and individual supervisors are responsible for monitoring inappropriate usage by NARA’s staff. However, an NA official stated there is no mechanism for allowing supervisors to view their staff’s internet activity. Furthermore, as described earlier, prior to NH generating the monthly blocked reports for NA and NGC, NARA’s web filter application was the only formal control in place.

In addition, the monthly reporting process continues to evolve, this is evidenced by the changing format and differing amounts of information reported from month to month. Also, the monthly reports are not consistently generated on a given date; some of the reports are generated weeks after the reporting period. The report currently lists NARA staff and their respective blocked attempt totals for each of the seven categories. NH has also at times included a list of the URLs making up the total blocked attempts for each user in a separate spreadsheet. This additional data provides a greater level of detail, however, it only includes the blocked attempts, it does not include the inappropriate sites accessed using [REDACTED]. Furthermore, up until now, the prevailing mentality has been that the sites on the blocked report were actually blocked, but our review discovered that in nearly all cases, if [REDACTED] the user is granted access.

The effectiveness of NARA 802 is further impacted as NA has not established formal procedures for reviewing the monthly report generated by NH. An NA official indicated they

review the list for egregious users, however no threshold has been established by NA to define what constitutes egregious inappropriate usage. Furthermore, NA focuses primarily on only two of the inappropriate categories: “Adult Material: Nudity” and “Adult Material: Sex.” Although NARA Directive 802 specifically prohibits gambling, it is not something NA has looked into even though past monthly reports have identified users who have consistently attempted, and likely accessed, gambling sites.

During the first five months of the new reporting procedure, NA had contacted one user’s supervisor in regards to inappropriate internet usage. However, during this timeframe there were multiple NARA employees who consistently showed up on the list with hundreds of blocked attempts in various inappropriate categories. In some of the samples reviewed, the monthly blocked attempt report is just the tip of the iceberg in terms of what inappropriate sites were actually accessed by NARA staff. Consequently, NA is only able to review information it is provided by NH. If NH does not fully embrace the monitoring tools available, NA will not have the information needed to fully enforce the policy.

Potential Impact of Not Fully Enforcing NARA Directive 802

NARA’s failure to fully enforce NARA Directive 802, as identified in this report, results in exposure to significant risks as outlined below:

- **Decreased Public Trust.** As mentioned earlier, Congress and the media have taken interest in the level of inappropriate internet usage by federal staff within the past year. As NARA continues to strive to address challenges facing its core goals, harmful distractions caused by inappropriate NARA staff internet usage must be avoided. NARA’s customers and stakeholders place enormous trust in NARA to fulfill its mission, as demonstrated at other federal agencies, inappropriate internet usage can negatively impact this trust and add doubt to the agency’s ability to meet its mission.
- **Reduced Employee Productivity.** NARA Directive 802 authorizes NARA staff to use the internet for personal reasons, provided it is during non-work time and does not interfere with official business or involve inappropriate use. NARA’s embrace of social media and networking tools is evidenced by the popularity of these sites accessed by NARA staff. However, if working on social networking tools does not fall within the NARA employee’s job function, hours spent on personal networking can negatively impact efficiency and job performance. Similarly, any time spent accessing inappropriate sites is time being taken away from NARA meeting its mission and providing timely services to its customers.
- **Legal Liability.** In accessing sexually explicit internet sites, NARA staff can contribute to creating a hostile work environment. When certain employees repeatedly access sexually explicit material in the workplace, others may be offended or uncomfortable and ultimately bring an action against the agency. This could

potentially lead to costs associated with defending the case, along with any resulting settlements or awards.

- **Degradation of Network Performance.** Excessive non-business use of the internet increases system exposure to viruses and malware and can cause degradation of network performance. Of particular concern are large video and graphic files often offered for download by sexually explicit sites. Network congestion can cost an organization not only in terms of slowed network performance, but also in the need to upgrade network resources.

Without the proper controls in place to ensure employee compliance with NARA Directive 802, NARA is at risk for continued employee abuse of the internet. NARA has taken important steps toward implementing the necessary tools to monitor and restrict inappropriate employee internet usage, including establishing appropriate use policy, installing a web filtering application, and establishing a process to generate monthly blocked attempt reports. However, NARA has not developed adequate procedures and devoted the resources necessary to fully enforce NARA Directive 802. NARA staff use a number of methods to bypass NARA's web filtering application, even though additional tools are readily available to NARA management to restrict inappropriate access. Further, the recently implemented reporting process does not provide the full detail of the inappropriate use taking place, and therefore disciplinary actions are not regularly pursued or enforced by NA.

Recommendations

1. We recommend NA, NH, and NGC work together to:
 - a. Develop an interdisciplinary team equipped to identify inappropriate use and address violations of NARA Directive 802 with suitable administrative action.
 - b. Establish a threshold of blocked attempts by individual users warranting further analysis for each NARA Directive 802 category.
 - c. Develop a monthly report format containing all the user activity for the NARA staff that surpasses the established blocked attempt thresholds.
 - d. Define formal roles and responsibilities in monitoring and analyzing the reports generated.
 - e. Establish formal criteria based on blocked attempts and successful access totals used to determine if supervisor notification and administrative action is appropriate.

2. We recommend NA provide notice to NARA staff that NA and NH are aware of web filter bypass methods in use (i.e., [REDACTED] etc.) and focus will be directed toward identifying violators and aggressively pursuing disciplinary action, up to and including removal.

3. We recommend NH work with the Websense contract staff on a regular basis to implement all available web filter application features and tools that assist with monitoring

and enforcing staff internet usage in accordance with NARA Directive 802. These include, but are not limited to:

- a. Generating a customized report identifying NARA users frequenting [REDACTED] [REDACTED] websites and analyzing the user activity to determine the extent of inappropriate usage.
 - b. Establishing keyword blocks based on inappropriate [REDACTED] accessed; these keyword blocks should be used to limit [REDACTED] accessible to NARA employees.
 - c. Determining the feasibility of real-time alerts in relaying inappropriate NARA staff internet usage to NA in order to provide the information in a timely manner.
 - d. Determining the feasibility of quota limits and time period features limiting the amount of time NARA staff can access non-work related websites throughout the workday.
4. We recommend NH develop a formal schedule to test Websense for intermittent failures and develop procedures for ensuring the web filtering application is reliable.
5. We recommend NH establish tests and procedures to ensure the Websense application at NARA field locations are uniformly configured and no systems are bypassing the web filter.

Management Response

Management concurred with the recommendations.

Appendix A – Example of [REDACTED] Accessed with no Web Filter Restriction

NARA staff are easily able to access inappropriate material posted [REDACTED] As shown below in an example of a site visited by a NARA employee, [REDACTED] itself has a warning page indicating the site may contain adult content. However, NARA currently does not provide restrictions [REDACTED] no matter what their content. [REDACTED] typically contain page after page of sexually explicit images.



Appendix B – Example of Web Filter Bypass

NARA staff made multiple attempts at accessing [REDACTED]. In the example below, one NARA user accessed [REDACTED] which lists a number of [REDACTED] that are not blocked by web filter applications. Once selected, the [REDACTED]. The example below shows a cropped portion of an adult site that is easily accessible via [REDACTED]. Although [REDACTED] may not be blocked by Websense, it still shows up on the user's web log, therefore, a review of the log can identify users accessing [REDACTED].



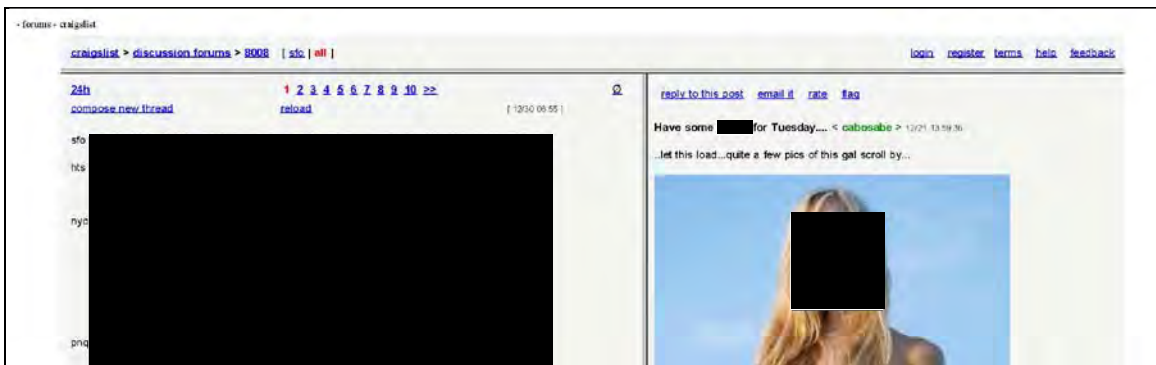
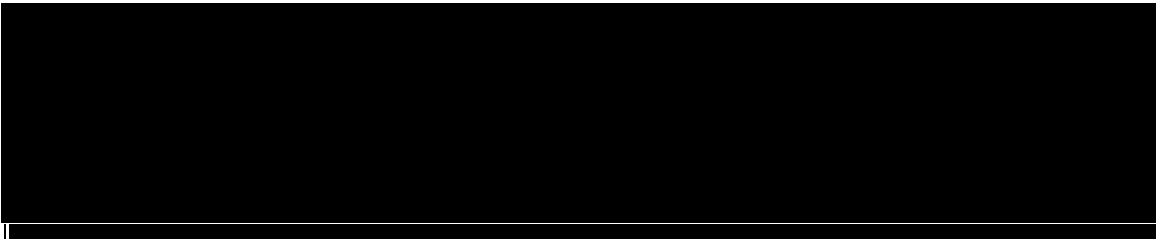
Appendix C – Example of a Site Accessed by [REDACTED]

A number of NARA staff [REDACTED] which based on our analysis typically resulted in the web filter application allowing access. Below is a screen shot of an [REDACTED] resulting in access to the page. “[REDACTED]” was frequented by one of the users sampled over 700 times during a three month period. The site contains sexually explicit videos and images.



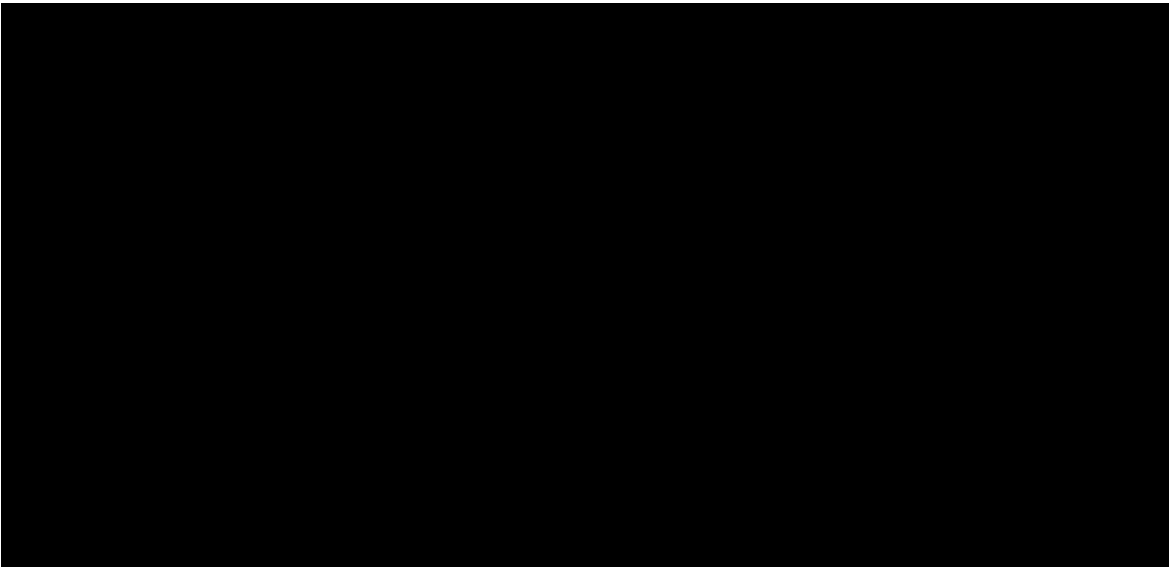
Appendix D – Example of Inappropriate Sites Accessible through Message Boards and Forums

One of the sampled NARA users visited a secret craigslist forum list “██████████” 72 times over a three month period, followed by thousands of forum visits. The Websense web filter application categorized this site and the sites accessed through it as ██████████ both of which are not blocked by the Websense application. A portion of a screenshot of “██████████” below gives an example of some of the numerous explicit forum topics available through the site. These forums often contain attached images of inappropriate material which are not typically blocked by the Websense application (a cropped version is shown below).



Appendix E – Example of Discrepancies in Sites Blocked across NARA’s Network

NARA users at field locations are not uniformly restricted from inappropriate websites. The example below shows the unrestricted access of the hack site [REDACTED] during a separate review at [REDACTED]. However, prior to the site visit, the same website was appropriately blocked at Archives II. This, as well as other examples shows inconsistencies among web filtering at various NARA locations.



Blocked by Websense



Your organization's Internet use policy restricts access to this web page at this time.

Reason: The Websense category "Hacking" is filtered.
[REDACTED]

Options:

Click [more information](#) to learn more about your access policy.

Click **Go Back** or use the browser's Back button to return to the previous page.

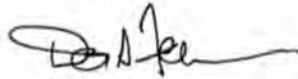
Appendix F – Management’s Response to the Report



Date: March 7, 2011
To: Paul Brachfeld, Inspector General
From: David S. Ferriero, Archivist of the United States
Subject: Audit Memorandum 11-10, Audit of Inappropriate Personal Use of the Internet at NARA

Thank you for the opportunity to comment on this draft report. The report includes five recommendations. We concur with all five recommendations and have already begun working to contain some of the problems noted in the draft report.

If you have questions about these comments, please contact Mary Drak at mary.drak@nara.gov or by phone at 301-837-1668.



David S. Ferriero
Archivist of the United States

NATIONAL ARCHIVES and
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

Appendix G - Report Distribution List

David S. Ferriero, Archivist of the United States (N)
Adrienne C. Thomas, Deputy Archivist of the United States (ND)
Rick Judson, Acting Assistant Archivist for Administration (NA)
Charles Piercy, Acting Assistant Archivist for Information Services (NH)
Gary M. Stern, General Counsel (NGC)
Steven Heaps, IT Policy Branch Chief (NHPL)
Mary Drak, Policy and Planning Staff (NPOL)