NATIONAL
ARCHIVES

OFFICE *of*
INSPECTOR GENERAL

Date : June 28, 2011

Reply to
Attn of : Office of Inspector General (OIG)

Subject : Management Letter OI 11-01: Unsupported [redacted]

To : David S. Ferriero, Archivist of the United States (N)

In December 2010, a complainant contacted OIG Office of Investigations to share a concern regarding the [redacted] used to [redacted] on NARA's network. Specifically, the complainant was concerned that [redacted] would no longer receive software updates including critical security updates. The OIG performed an inquiry into this matter to (1) determine the facts surrounding [redacted] (2) assess the potential effects resulting from the use of unsupported [redacted] (3) determine what steps NARA has taken to address risks resulting from the use of unsupported [redacted] (4) determine factors that contributed to NARA's continued use of unsupported [redacted] and (5) determine steps that NARA is taking to replace software including timeframes for deployment of replacement software.

The purpose of this management letter is to formally advise you of the results of that inquiry. The claim was substantiated in that we found [redacted] for [redacted], and the vast majority of PCs connected to the NARA network use this [redacted]. As a result, software updates including critical security updates from [redacted] are not being applied to these PCs. We found that management in the Office of Information Services (NH)[1] has been aware of this condition for some time and that, while some steps have been taken to mitigate the increased risk resulting from this condition, a replacement [redacted] has not yet been identified. On April 7, 2011, we sent an email message to the Deputy Chief Information Officer (DCIO), requesting additional information about this matter. On April 13, 2011, we received a written response from the DCIO. We have referenced responses to our questions in this management letter where appropriate and have attached a complete copy of the DCIO's response.

---

[1] Issues identified in this management letter initially arose prior to the agency-wide reorganization. Thus, a determination was made to employ acronyms and titles which existed at that time.

Majority of workstations connected to the NARA network use [redacted] that is no longer supported by the manufacturer

In early [redacted] reported that support for the [redacted]. In the period leading up to the end of support date, [redacted] repeatedly reminded users that support would be ending and encouraged users to either upgrade to the [redacted] or [redacted] as soon as possible. [redacted] formally discontinued support for the [redacted] on [redacted] In the [redacted] on that date, [redacted] stated that [redacted]

We used [redacted] a network management tool installed on the NARA network, to determine if workstations connected to the network are using the [redacted] and, if so, how many PCs are using [redacted] We discovered that the vast majority of workstations connected to NARA network are using the [redacted]. In fact, as of June 13, 2011, the [redacted] reports that NARA has almost five-thousand workstations deployed. For these workstations, [redacted] reports that four-thousand seven hundred and nine (4,709) of the workstations use the unsupported [redacted], that two-hundred sixteen (216) workstations use the [redacted], and that two (2) use the [redacted]

Use of an unsupported operating system increases risk to the network

The primary concern expressed by the complainant is that, since PCs connected to the NARA network are using [redacted], these workstations would no longer receive software updates. Software updates frequently include critical security updates that patch known vulnerabilities and can help protect computers from [redacted] and [redacted]. As a result, it has long been accepted in the IT security field that applying patches to systems is one of the most effective ways of reducing the risk of malware incidents and that many instances of malware have succeeded because systems were not patched in a timely manner.

We used [redacted] to examine the state of patch application on PCs connected to the network. We discovered that, in the period leading up to [redacted] PCs on the network were generally receiving patches that were categorized as critical security updates for [redacted] In fact, the [redacted] patch that was released by [redacted] was applied to four-thousand seven-hundred and forty eight (4,748) of the PCs connected to the network and was not applied to fifty-five (55) workstations. After that date, we identified a sharp drop-off of patches being applied to PCs connected to the network. For example, on [redacted] released the [redacted] to address a [redacted] that could allow [redacted] In the executive summary description for this patch, [redacted] Although it was known that this

vulnerability affected PCs using the [redacted] did not release a patch for [redacted] We used [redacted] to determine the extent to which this critical patch was applied. We discovered that the patch was applied to just one-hundred thirty four (134) PCs connected to the network. We identified thirty-six patches identified as critical security updates for [redacted] in [redacted] since [redacted] support for [redacted] and did not identify any instance in which more than one-hundred seventy-two (172) PCs connected to the NARA network received the patch.

We requested information on risk mitigation in our questions to the DCIO. In his response, the DCIO reported that NH has taken several steps to address the additional risks including developing an [redacted] mitigation strategy, upgrading all public access PCs to [redacted] and continuing to review the matter on a weekly basis. With respect to specific critical patches, the DCIO provided the following information:

> "Since [redacted] went out of support, [redacted] critical patches[2] have been released. Since these patches address vulnerabilities to [redacted], they may not all apply to our environment. NITTSS has a process to review the patch releases for remediation strategies in our environment. Mitigation strategies have been applied to remediate vulnerabilities for [redacted] of the patch releases. Possible workarounds have been identified for [redacted] others, but need to be reviewed for business impact before moving forward with the remediation. The remaining workarounds would have an unacceptable impact to the functionality and NARA is accepting the risk."

NH is considering options for replacing the unsupported [redacted]

As part of this inquiry, we requested information on the planning process related to the replacement of the [redacted] At the time of our inquiry in late [redacted], we were informed that a test plan had been prepared to evaluate [redacted] and [redacted] as possible replacements for [redacted] but that testing had not started. We were also advised that testing would take approximately [redacted] to complete (meaning that testing would be completed in [redacted]) and that a technical recommendation would be provided to the Technical Review Group at the completion of testing.

NH Management has delayed the selection and deployment of a supported [redacted] because of other priorities

In our request for information from the DCIO, we asked why it has taken NARA so long to plan for the replacement of [redacted] In his response, the DCIO explained that planning started late in [redacted] and has been ongoing since that time. The DCIO recounted several instances in which NH management considered upgrading [redacted] from [redacted] and made the decision not to take action. We asked if NARA considered upgrading to [redacted] when it was released in [redacted]

---

2 It should be noted that we did not attempt to reconcile the number of critical patches that we identified in our examination of [redacted] ([redacted] critical patches) with the number of critical patches reported by the Deputy CIO in his response ([redacted] critical patches). Further, we did perform additional research as part of this inquiry into the remediation strategy employed by NH as described in the Deputy CIO's response.

[redacted] and received the following response:

> "The Office of Information Services (NH) has a fundamental assumption with regard to managing risk that is outlined in NARA's Enterprise Architecture (EA). Specifically, Assumption 1 – We will manage IT risk with the rationale being that '... NARA prefers a conservative approach to IT system deployment ...' and 'NARA generally does not want to be an early adopter of new technologies ...' However, NH did consider upgrading to [redacted] in [redacted] as part of the PC refresh project. This was reviewed with the NH TRG on [redacted]. However, at this point it was still generally considered too early to deploy [redacted] due to concerns about the initial release of [redacted] and the impact it would have on some of our critical business applications because of known issues with [redacted] "

We were also informed in the DCIO's response that a number of other priority projects were ongoing during this timeframe including [redacted] upgrade.

Conclusion

We determined that the vast majority of PCs connected to the NARA network use the [redacted] We confirmed that [redacted] is no longer [redacted] and, as a result, PCs using [redacted] no longer receive software updates [redacted] including critical security updates. We determined that PCs that do not receive security updates are at an increased risk from [redacted] We determined that NH has taken steps to mitigate the increased risk, but we question the timeliness and effectiveness of an internal remediation process as compared to regular security updates from [redacted] NH management reported that they are taking steps to evaluate possible replacements for [redacted] but that no decision has been made on a replacement [redacted]. We were advised that the evaluation process will not be completed until [redacted]. We were informed by NH management that they have been planning for the replacement of the [redacted] for almost [redacted] but have delayed the selection and implementation of a replacement [redacted] because of concerns about the impact of a new [redacted] in our environment and because of other priorities.

I have referred this issue to my Office of Audit for consideration as part of the audit planning process. Should you have any questions or require any additional information about this matter after you have had an opportunity to review this management letter, please e-mail me or Ross Weiland, AIGI, or call us at (301) 837-3000.

Paul Brachfeld
Inspector General

The attachment to Management Letter OI 11-01 has been redacted in full.