

**TO:** Appraisal Subcommittee

**FROM:** Jim Park, Executive Director

**DATE:** December 1, 2022

**RE:** December 7, 2022 ASC Briefing Package

---

This should be the last Briefing/Meeting on Zoom. We are finalizing an agreement with Webex to move to that platform. We will plan testing to ensure that all members are able to successfully use Webex.

Explanation of Agenda Items:

ASC Hearing Update/Discussion

- Discuss the January 24 Hearing (10:00 – 12:00), Save the Date, Working Group, etc.

Website/PII Breach Update

- Discuss the After Action Report and next steps

TAF Audit

- Discuss close out of TAF 2017-19 Grants Audit

TAF Board Resignations

- Discuss recent communication to ASC Board Members

Staffing Update

- Update on Grants Director, General Counsel and Regulatory Affairs positions
- Proposed staff reorganization to be discussed at a later date

Other Business

- Opportunity for Board and staff to discuss other topics (as time allows)

# **December 7, 2022**

# **Briefing Agenda**

## Briefing Agenda

**Date:** December 7, 2022

**Time:** 10:00 a.m. ET

**Location:** Go to the Link below to register for the Briefing:

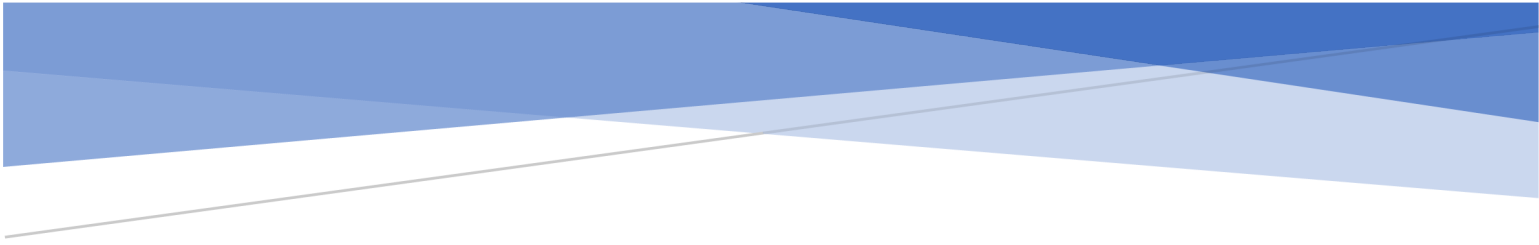
<https://www.zoomgov.com/meeting/register/vJItde2upjMiHvCqbA2M5C5CbiP5QD-1YtU>

| Briefing Topic(s)                    |                               |                      |
|--------------------------------------|-------------------------------|----------------------|
| <b>Opening Remarks</b>               | <b>Chair Martinez</b>         | <b>10:00 – 10:05</b> |
| <b>ASC Hearing Update/Discussion</b> | <b>Chair Martinez</b>         | <b>10:05 - 10:25</b> |
| <b>Website/PII Breach Update</b>     | <b>J. Park/A. Ritter</b>      | <b>10:25 - 10:45</b> |
| <b>TAF Audit</b>                     | <b>J. Park</b>                | <b>10:45 – 11:00</b> |
| <b>TAF Board Resignations</b>        | <b>J. Park</b>                | <b>11:00 – 11:15</b> |
| <b>Staffing Update</b>               | <b>J. Park</b>                | <b>11:15 – 11:25</b> |
| <b>Other Business</b>                | <b>Chair Martinez/J. Park</b> | <b>11:25 – 11:30</b> |

# **After Action Report**

# **Findings prepared by**

# **NDI**



After Action Report  
Findings Concerning PII Data Leak  
Prepared for  
Appraisal Subcommittee Appraisal Subcommittee (ASC)  
Federal Financial Institutions Examination Council  
(FFIEC)  
November 30, 2022

**Abstract**

This report presents the findings related to a minor Personally Identifiable Information (PII) exposure that occurred October 13, 2022, during the launch of the new [www.ASC.gov](http://www.ASC.gov) website.

# After Action Report

## Personally Identifiable Information (PII) Data Leak

### Executive Summary

This report presents the findings related to a Personally Identifiable Information (PII) exposure that occurred after the conversion and launch of the new Appraisal Subcommittee (ASC) website [www.ASC.gov](http://www.ASC.gov) (ASC website) that hosts the ASC National Registries.

NDi launched the new ASC website on September 19, 2022. On October 13, 2022, an appraiser noticed that his Appraiser Identification Number (Appraiser ID) was visible on the internet. The Appraiser ID (mandated by the State) is their personal Social Security Number (SSN). ASC is aware that some States use the appraiser's SSN for the appraiser's unique digital ID within the ASC Registry and has requested that these States not use SSN as a unique digital ID, but the States have not complied with this request. NDi developed an encryption module to encrypt this data before ingesting it into the ASC website, but ASC has not been able to implement this solution either. ASC currently holds approximately 330,000 appraiser records within the ASC Registry database, and within those records there are approximately 4,800 SSNs that were potentially exposed. All 330,000 appraiser records contain PII consisting of the full name, telephone numbers, and address of the appraisers, but this PII has been approved by ASC for publication in the National Registries.

On October 13, 2022, ASC informed NDi that an Appraiser ID was visible on the internet and directed NDi to take the ASC website offline and update the website to block the Appraiser ID from being displayed. The website was down for approximately 24 hours while the remediation and updates were performed. The website was brought back online on October 14, 2022. As a result, and based on the forensic review performed thereafter, the only known exposure of SSN data occurred when the individual appraiser reviewed his own record.

This report will present the nature of the data leak and why it occurred. This report will also assess the impact of the data leak and provide recommendations to ASC on improvements that can be made to the ASC website to prevent future data leaks or malicious hacks.

### Background

ASC contracted with Network Designs, Inc. (NDi) to provide various information technology (IT) support services. The base contract was awarded per GSA Schedule 70 Terms and Conditions. The specific work efforts are initiated as Task Orders using Time and Material (T&M) estimated hours to complete each Task Order. ASC engaged NDi to design, develop and deploy a "new" ASC website using the Drupal Content Management System (CMS), which is open-source software (i.e., free software with no corporate entity for support). Open-source software is developed by a community of individual users versus a company and relies on this developer user community for support. The Drupal CMS is used by ASC and the development staff to create, manage, and publish material on the ASC website. Ultimately the exposure of the Appraisal ID was due to a configuration issue within the Drupal CMS.

## ASC Information Technology Infrastructure Issues

**Server hosting:** ASC provides and maintains servers at a single data center located in Silver Spring, MD. Multiple servers support the web, database, and CMS applications. This site represents a single point of failure for the ASC website and National Registries. Current industry best practices for server hosting include using cloud services for all mission-critical systems versus owning and operating individual servers. Cloud services are easier to maintain and provide a more robust, reliable, and secure system than servers owned and operated by ASC.

Buying a cloud provider's compute and infrastructure services also helps to defray significant capital expenses when updating and modernizing IT systems. Unfortunately, ASC has been unable to properly modernize its IT systems and has had to defer updating critical components and systems. This results in "technical debt" that relentlessly accrues, taking an ever-increasing portion of the IT budget to support baseline operations that cripples efforts to innovate and modernize. The data center in Silver Spring represents a single point of failure which is compounded by an antiquated system architecture that is brittle (i.e., catastrophically breaks because of minor changes), difficult to support, and not based on industry best practices. ASC also provides the development and testing environments, which are inadequate to effectively develop, test, and secure the ASC systems. The existing development and test environments are difficult to expand due to the significant capital outlays required to update the hardware, software and tools in those environments.

**Practices and procedures:** ASC has not implemented industry best practices for website development, operations, and security management. Industry best practices combine Development, Security, and Operations into one continuous practice, DevSecOps, which enables effective development and oversight of the systems, servers, and applications required to run a website. DevSecOps does this by ensuring that development efforts provide necessary capabilities; that these required capabilities are operationally implemented in a controlled manner; and that security is introduced as early as possible into the system lifecycle. DevSecOps involves standing up development and testing environments that can fully simulate all aspects of the operational website and can automatically move updated code from the development environment to testing and eventually into operations, minimizing human errors during this process.

**Drupal:** Using open-source software such as Drupal CMS requires active and continuous participation in the open-source community to ensure the product is appropriately implemented and maintained. NDi advised ASC against using Drupal CMS due to several factors, including the lack of a centralized support structure, lack of funding to ensure proper participation in the open-source community, general maintenance concerns, and overall product complexity. In addition, Drupal is a popular CMS with many advanced features requiring significant expertise to use effectively. Despite NDi's concerns, ASC directed NDi to use Drupal CMS technology in developing the new ASC website.

**Database Architecture:** The ASC website interfaces with the ASC National Registry based on legacy SQL database technology (i.e., backend) initially developed for ASC in the 2008 timeframe. This legacy database design and architecture were not updated to best support the Drupal CMS, making the system less secure and more brittle. Critical functionality was moved from the SQL server to Drupal CMS to save time, and money led to the data leak. The ASC SQL database server is a central component in the ASC application architecture, and the interactions between Drupal and the SQL server do not appear to have the capacity to meet all of the ASC performance requirements for queries and appraiser data ingestion.

The ASC SQL server also represents a single point of failure, and data is not encrypted within the ASC SQL server.

**PII Data Management:** NDi recommended to ASC that the States encrypt the appraiser IDs that are also the appraiser's SSN before ingestion into the National Registries. NDi developed an encryption tool for this purpose, but ASC could not mandate the states to comply with this recommendation. Rearchitecting the database solution in a robust DevSecOps environment would have allowed the NDi development team to detect this potential exposure before the system was put into operation and implement the proper security controls to prevent exposure.

## Data within the National Registries

The data used by the ASC website resides within two "registries" known as the Appraisal Registry and the Appraisal Management Companies (AMC) Registry. Collectively they are referred to as the National Registries. The National Registries list certified and licensed appraisers and registered Appraisal Management Companies (AMCs). The States authorize these individuals and organizations to perform appraisals concerning federally related transactions. The National Registries are stored on the ASC legacy SQL server and accessed via the ASC website.

The Appraisal Registry consists of 330,000 records for individual appraisers. It includes data such as the appraiser's credentials, the status of their credentials, and PII data such as phone numbers, addresses, and occasionally SSNs for each appraiser. The AMC Registry stores similar information but for appraisal companies. The ASC website provides a "Search" capability for the public to find information about specific appraisers and AMCs stored within the National Registries. The individual state agencies have regulatory responsibility over appraisers and AMCs and regularly submit updates to the National Registries concerning such issues as disciplinary actions against expired appraiser licenses, certifications, expired AMC registrations, and updates to addresses and phone numbers.

The participating States submit/upload their appraiser and AMC information to the National Registries at least monthly. Against the recommendations of NDi and ASC, several States continue to use appraisers' Social Security Numbers (SSN) as the unique identifier for the digital records they upload to the ASC Registry, which is problematic. Because there is no standard for how States and Territories define the digital identifier of appraisers (appraiser ID), the ASC Registry must hold SSN data within the SQL database. The SSN is not required by ASC, so ASC should not collect and maintain SSNs.

The ASC website contains and publishes other (non-SSN and non-sensitive) PII information from individual appraisers, including names, addresses, and telephone numbers. While regulations require ASC to collect and publish this data, better controls on this data need to be implemented to ensure data moves, adds, deletions, and changes are quickly implemented without error.

## ASC Website Development and Testing

On October 1, 2021, NDi began designing and developing the new ASC website, including converting the intranet and extranet websites to the Drupal CMS and integrating with the legacy SQL Server hosting the National Registries. After a period of development using an agile development approach, a test version of the ASC website was delivered to ASC in February 2022 for User Acceptance Testing (UAT). UAT is intended to act as a final verification of the required business functionality and proper functioning of the system



(i.e., the ASC website) before the system is put into production. ASC has full responsibility for UAT and did not identify any operational or security concerns during UAT.

The potential data leak should have been identified during UAT. Still, the data leak was due to the lack of thorough testing processes, standard testing tools, and a testing environment adequate to simulate the operational ASC website. Load and stress testing should also have been performed prior to the site going live, but ASC does not have the tools or staffing required to perform this type of testing. Performance issues cannot be identified proactively in the current ASC on-premise hosting environment resulting in risky deployments of new code.

## Timeline of the Data Leak

September 18, 2022, 9:00 AM: ASC directed NDi to go live or launch the "new" ASC website effective September 19, 2022, at 12:00 a.m.

October 13, 2022, 9:37 AM: NDi was notified that a user of the ASC.gov website reported that he/she was able to view his/her Social Security Number (SSN) in clear text on a webpage served by the ASC website.

October 13, 2022, 9:45 AM.: NDi's Project Manager (PM) was asked to join an emergency ASC MS Teams call where she was notified of the PII exposure. Subsequently, the ASC IT PM directed NDi PM via email to take the ASC website down and display "Site Under Maintenance" page.

October 13, 2022, 10:12 AM: NDi took the ASC website offline and replaced it with a web landing page showing "Site Under Maintenance." At 10:21 AM, NDi notified the ASC IT manager that the site was confirmed offline with the splash screen in place.

The total elapsed time from notice of the incident to corrective action was approximately **35 minutes**. The total time the ASC website was potentially vulnerable to PII exposures was the period from site launch on Sept 19, 2022, to October 13, 2022.

## Incident Response

October 13, 2022, 4:30 PM: As noted above, NDi immediately began a forensic analysis of the website code and backend SQL Server database. NDi developers quickly confirmed that the condition that allowed the incident was within the Drupal CMS. NDi developers made corrective code configurations and software script changes within Drupal CMS to ensure that Nodes (the type of page exposed in this incident) cannot be reached by navigating the website. NDi requested Google to clear/remove existing ASC.gov web pages from Google Search indexes.

After determining the type of data exposed by the single reported user exposure, NDi then performed standard database queries of the ASC Registry SQL Database to determine that the total number of appraiser records that contain SSN data is 4,808. There is no indication that any other 4,808 records were accessed or viewed except for the single user access of their information that is the subject of this incident. NDi continues to review Google Analytics to retrieve data specific to this event to understand how many potential page views occurred in particular to this incident.

As stated above, the direct node access functions of Drupal CMS were disabled for the entire site, and the data field of the record that showed the SSNs was masked and is no longer displayed. The corrective

actions were completed within the first 24 hours from the notice of the incident. NDi PM then notified ASC leadership that ASC.gov website was secure and ready to go back online.

October 14, 2022, 12:18 PM: ASC requested that the ASC website be brought online. At 12:35 PM on 10/14, NDi confirmed that ASC.gov was back online and fully operational. The total time the ASC website was offline was approximately 26 hours.

## How Did it Happen?

The cause of this minor, non-malicious data leak is that the Drupal CMS was incorrectly configured to display the Appraiser ID. This configuration issue was not identified during development or ASC's UAT testing but was detected by a single appraiser looking at their data record.

## Why Did it Happen?

This data leak was a direct result of some States sending ASC appraiser data that contains SSNs and the lack of proper controls to prevent this data from being exposed on the website. NDi had recommended that the States encrypt this data – and ASC agreed and contracted with NDi to develop a software tool to encrypt this data. However, ASC could not compel the States to use the tool resulting in the continued ingestion of SSN data into the ASC Registry. The website was configured to display the appraiser ID, and for most of the appraisers, this is fine, but for States sending SSN data to ASC, this resulted in a single SSN exposure.

The lack of an industry-standard DevSecOps environment and associated practices allowed this flaw to propagate from development to testing and eventually to operations without being detected. As noted above, ASC was responsible for testing the new website. Multiple failures occurred, resulting in the data leak: failure to prevent SSN data from entering the ASC database, inability to protect the SSN data once ingested in the ASC systems, and failure to detect the accidental exposure of SSN information during testing.

## Conclusion

Based on our analysis of the available information and forensic sources (i.e., audit logs of the Registry SQL Database, ASC.gov Drupal CMS code, and Google Search and Analytics), we did not detect any malicious or unauthorized use of the information that was briefly exposed. Therefore, we believe this incident is better characterized as a system vulnerability that quickly closed once detected and represents a "near-miss" rather than a data breach.

There is no evidence that any harm to any individual or company has occurred through this data leak. Although minor, the incident was not taken lightly by NDi, which immediately corrected the issue, commenced forensic analysis, and initiated discussions with ASC concerning implementing more rigorous security controls and a more secure data architecture.

## Recommendations

To prevent future data leaks and to ensure the ASC website meets ASC objectives, ASC should undertake the following actions to the ASC systems and overall architecture:

Architecture Update: The ASC Registry is outdated technology, and the architecture business rules of the SQL Database should be updated using industry best practices to define the overall architecture of the ASC Extranet, ASC Intranet, ASC website, and National Registries.

Move to Cloud: Rearchitect the ASC Registry database and website, servers, and applications to leverage cloud technologies and exit the Silver Spring data center. Specifically, the ASC Registry and all ASC IT infrastructure should be moved to a cloud platform (i.e., AWS or AZURE) from the current hosting facility. Standup development and testing environments in the cloud equipped with the appropriate tools, processes, and resources.

DevSecOps: ASC should update its IT development environments in the Cloud to include DevSecOps processes and update its data-security management policies and procedures for all data used by the ASC website.

Data Storage: NDi recommends that since the Appraisal Registry contains PII data, the data should be explicitly protected at rest and in use. If ASC continues to accept appraiser records from States that use SSN as the unique identifier for the appraiser record, there will be inherent risk associated with the storage of this data on ASC servers. ASC should implement encryption technologies to secure the Registry data at rest and in transit. Registry data in use protections should include robust access controls and user access auditing.

System Monitoring and Data Leak Detection: ASC has no technologies to detect inappropriate data disclosures. A good data security architecture should be multi-layered, including detecting and notification of security issues and events. NDi recommends implementing a data inspection appliance such as the Barracuda Data Inspector to monitor the data entering and leaving the ASC website. Such an appliance provides insight into sensitive data (i.e., SSN), can find and block malware before it is activated, and help ASC identify and quantify all data contained within the National Registries to ensure ongoing compliance with all security and regulatory guidance.

CI/CD: An updated system architecture that supports Continuous Integration / Continuous Delivery (CI/CD) will best address current ASC website operational issues and enable the safe integration of new requirements going forward. Deploy automation that enables CI/CD of capabilities to the ASC website and associated systems using a DevSecOps methodology.

Note that ASC's contract with NDi does not call for the above recommendations and ASC would need a new contract vehicle to implement them.

# **TAF Audit Management Decision**

TO: Dave Bunton, President, Appraisal Foundation

FROM: Jim Park, ASC Executive Director

DATE: November 17, 2022

RE: Management Decision on Audit Report of the 2017-2019 Appraisal Foundation Grants

---

This Management Decision is issued on the Performance Audit Report of McBride, Lock & Associates, LLC dated July 2022: “Administration of Payments Received from the Appraisal Subcommittee [ASC] by The Appraisal Foundation [TAF]” (Report).

The auditors recommended that TAF:

- a) Determine the total funds expended in creating the USPAP for fiscal year 2017, 2018, and 2019, and
- b) Create an allocation method and determine the amount of funds which is program income for each fiscal year 2017, 2018, and 2019, and
- c) Work with ASC to determine the appropriate resolution of funds which would be questioned costs for not properly accounting for program income, . . .

The auditors also recommended that the ASC implement procedures to ensure that all program income is properly accounted for and utilized in future Federal grants.<sup>1</sup> The auditor’s recommendations are predicated on application of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance) at 2 CFR Part 200 (Super Circular) to the grants administered by the ASC during the audit period of fiscal years 2017 – 2019.

TAF submitted a response to the Report dated June 17, 2022, which incorporated by reference TAF’s response to the Finding dated December 9, 2021. The responses to the Report and the Finding are attached.

---

<sup>1</sup> Auditor’s Report at page 5.

Pursuant to Title XI of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (Title XI), the ASC is authorized “to make grants in such amounts as [the ASC] deems appropriate to [TAF], to help defray those costs of the foundation relating to the activities of its Appraisal Standards and Appraiser Qualification Boards.”<sup>2</sup> Beginning in 1996, ASC grants to TAF were administered through the U.S. General Services Administration (GSA) as an Order for Supplies and Services (GSA Form 300) and treated as a contract, without any reference to application of the Super Circular, which includes specific requirements for both grantees and grantors. Specifically, 2 CFR 1.305 requires a federal agency to issue and appropriately implement necessary guidance in order for the grantee to be subject to the provisions of the Super Circular.

With the ASC’s budget increasing and grant authority expanded, in December 2019, the ASC adopted a comprehensive Grants Handbook, which included adoption of the Super Circular. The adoption of the Grants Handbook and Super Circular significantly changed the process for administration of ASC grant funding beginning in 2020.

In conclusion, guidance from the ASC which would have triggered application of the Super Circular was not adopted until December 2019. Therefore, the recommended action in the Report to account for program income is not applicable to the audit period of fiscal years 2017 – 2019. The ASC addressed the auditor’s recommendation to “[i]mplement procedures to ensure that all program income is properly accounted for and utilized in future Federal grants,” in its adoption of the Grants Handbook and Super Circular in December 2019.

## Attachments

---

<sup>2</sup> Title XI § 1109 (b)(4), 12 U.S.C. § 3338 (b)(4).