Internal Audit Department

IT Security Audit:
Internet Domain/Subdomain and Email Management

August 17, 2021
Revised August 19, 2021
Report Number FY 21-04

Distribution:
Audit Committee, Arizona Board of Regents
Internal Audit Review Board
José Luis Cruz Rivera, President
Steve Burrell, Chief Information Officer, Vice President, Information Technology Services
Don Carter, Director, ITS Academic & Research Technology Services
Ann Marie deWees, Associate Vice President, University Marketing
Bjorn Flugstad, Vice President, Finance, Institutional Planning and Analysis
Kyrie Fry, Assistant Director, University Marketing
Michelle Parker, General Counsel
Andrea Stalker, Director, ITS Strategic Planning, Implementation & Education Services
Wendy Swartz, Associate Vice President and Comptroller
Harlan Teller, Chief Marketing Officer
Matthew Wall, Director, University Marketing
Daniel Wallace, Manager, ITS Information Security Services
PJ Way, Director, ITS Infrastructure & Platform Services
Brett West, Associate Director, ITS Infrastructure & Platform Services
Michael Zimmer, Director, ITS Information Security Services

This report is intended for the information and use of the Arizona Board of Regents, NAU administration, the Arizona Office of the Auditor General, and federal awarding agencies and subrecipients.
Summary

Audit of IT Security is in the Annual Audit Plan for Fiscal Year 2021 (FY21), as approved by the Audit Committee of the Arizona Board of Regents (ABOR). This audit supports Northern Arizona University's (NAU / University) strategic goals of Student Success & Access and Stewardship by ensuring domains and subdomains are adequately managed and represent consistent NAU brand recognition through internet web presence, ensuring security technologies adequately support and enhance the trust in University electronic mail (email) communications, and ensuring email communications comply with applicable laws, rules, and regulations.

Background:

NAU uses various approaches and services to market and communicate with prospective and current students, parents, alumni, donors, other consumers of NAU's various services, and faculty and staff from other organizations. Whether through paid advertising, media relations, brochures, or other printed publications, promotional videos, commercials, internet webpages, direct mail, email, social media or other means, the consistent application of strategies to promote and protect the NAU brand is of key importance. Safeguarding the NAU brand and increasing brand recognition and reputation includes ensuring electronic communications are trusted and successfully delivered / presented to intended recipients. Effective marketing and related communications involve mass marketing email campaigns and NAU’s internet web presence.

Like brick-and-mortar store fronts, good internet domain / subdomain naming and structure is important since the first research most individuals conduct when seeking information about higher education institutions is to complete an internet search. If the website is easy to find and navigate, the potential for attracting students and other constituents likely increases. An internet domain name is a unique name assigned to an entity or person with an established presence on the internet, and that requires formal registration. The name is combined with a generic top-level domain, such as .com, .edu, or .org. Internet subdomains can be created as desired (no required registration) by the domain name owner and are typically reflected as a prefix added to an existing top-level domain name to help with the organization and navigation of the related internet presence. Thus, NAU’s top-level domain, NAU.EDU, includes many subdomains, such as IN.NAU.EDU representing NAU’s primary internally facing web presence. Domains and subdomains can be further organized into subdirectories like IN.NAU.EDU/ITS/ (NAU Information Technology Services website).

Email communications are routinely distributed to a wide audience, including international students, and mass marketing platforms provide the most efficient, cost-effective way to communicate NAU’s benefits, including ground-breaking research, community events, academic and student successes, and athletic events. These efforts involve both mass marketing email campaigns and NAU’s internet web presence. Ensuring the effectiveness and deliverability of these campaigns is important to maintaining and increasing student enrollment.

Email authentication technologies provide greater assurance on the identity of the sender of a message, thereby helping to ensure that NAU emails are not routed to spam or junk by the recipient email service, or to prevent emails from being “spoofed” to create fraudulent email messages from authorized NAU email accounts. Domain-based Message Authentication, Reporting and Conformance (DMARC) protocols help email receivers determine if messages align with what
receivers know about senders. (See Exhibit A for additional details, including a more in-depth summary of the email authentication process and DMARC best practices for email deliverability management).

**Audit Objectives:** The primary audit objectives were to 1) assess the extent the University maintains and monitors its internet domains and / or subdomains; 2) ensure best practice email management and security protocols are implemented to limit exposure to external attacks; 3) ensure email deliverability that allows recipients to identify authenticated NAU email communications; and 4) determine if the University’s email communications support compliance with federal and state laws, rules, and regulations.

**Scope:** Establishing the audit scope included working with management to identify high-risk cybersecurity matters, reviewing Information Technology Services (ITS) procedures for purchasing software, including Software as a Service (SaaS), reviewing policies and procedures to understand approaches to ensuring compliance with federal and state laws, rules and regulations, and evaluating the results of information technology security related internal and external audit work completed over the past three years. As a result of this effort, we concluded that the management of internet domains and subdomains and the management of email communications presented potential information security and business challenges that have not been otherwise addressed.

We focused our work on gaining an understanding of related NAU activities by identifying the following as of May 31, 2021:

- How NAU has structured its primary internet domain (NAU.EDU) and the related subdomains that make up NAU's internet / web presence.
- The departments, units and functions that use email to market NAU programs and services to prospective students, parents, alumni, donors, and constituents.
- The applications and / or services used to create and manage email marketing campaigns.
- If and how well the third-party email applications and / or services used by NAU to authenticate emails, ensure messages are delivered to intended recipients’ email inboxes.

We conducted such analyses, tests, and other procedures as we deemed necessary to address the audit objectives.

**Methodology:** The following procedures were performed to accomplish the audit objectives:

- Worked with NAU ITS Information Security Services and University Marketing staff to identify the specific objectives, risks, and controls related to the management of email and internet domains and subdomains. This included review of a preliminary DMARC analysis completed by the Information Security Services team.
- Reviewed security procedures for University-owned and registered internet domains and subdomains to ensure Domain Name System (DNS) records are properly configured and managed.
- Reviewed DMARC authentication reports and identified departments using:
  - Third-party marketing platforms with failing email authentication services.
  - Software applications with failing email authentication services.
- Reviewed FY21 ITS software inventory lists, ITS Checklist Status reports, and procurement card (PCard) transactions to identify NAU colleges, departments, units, and functions using third-party marketing platforms for mass email communications.
- Worked with University Marketing staff, ITS staff, and third-party application vendors to obtain
Canonical Name (CNAME) records and implement protocols to decrease DMARC failures.

- Monitored DMARC status for proper alignment after implementing protocols and communicated improvements to NAU departments.
- Reviewed third-party marketing platform privacy policies.
- Interviewed staff and reviewed supporting marketing communications to verify compliance with federal and state regulations, and University procedures related to email marketing.

Reviewed the federal CAN-SPAM Act, Arizona Revised Statutes (A.R.S.), and ABOR and NAU policies and procedures related to IT Security.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing promulgated by the Institute of Internal Auditors* and accordingly, included such tests considered necessary under the circumstances.

**Conclusion:**

NAU's internet domain / subdomain structure and its mass email marketing approaches have evolved over many years starting at a time before its notable enrollment growth and before protocols like DMARC authentication became a reality. Since no obvious problems had been identified and restructuring internet domains / subdomains and email authentication requires collaboration with other administrative and academic departments, especially including University Marketing, making such notable changes has not been a priority over other critical business and IT needs. As a result, the NAU internet domain / subdomain and email authentication policies, procedures and processes could be better aligned to support NAU's strategic direction.

However, through a combination of IT centralization and maturation over recent years, identification of the need for a more formal and organized approach was identified, resulting in collaboration among ITS, University Marketing and Internal Audit to assess the current state of domain and email management to help identify areas for focused improvement. ITS and University Marketing are now better aligned to improve management of these areas going forward to the benefit of all related NAU Community stakeholders. Changes in the application of email authentication protocols have already demonstrated improvements in email deliverability and the related security of email communications.

ITS and University Marketing have established solutions that should result in continued short-term improvement while plans for domain and subdomain restructuring are developed, matured, and implemented. Expansion of the existing Web Advisory Council membership and inclusive approach to web governance should result in additional ongoing improvement, including creating and or improving policies and procedures reflecting shared responsibilities for:

- Establishing uniform web standards for all NAU web pages, including web pages directly related to NAU business and academic activities;
- Recording, registering, renewing, and managing the University’s domain name assets;
- Establishing electronic communication as the official means of University communication and parameters for use; and,
- Establishing parameters for the University’s mass email communications process and approvals.
Observations:

- University Marketing is expanding the Web Advisory Council membership to include ITS Infrastructure & Platform Services and/or ITS Academic & Research Technology Services (ARTS) representation. University Marketing is also working on a website redesign project to ensure NAU branding and logos are consistent across the NAU web platform; and, ITS Infrastructure & Platform Services is also considering development of a ServiceNow repository to create workflows between University Marketing and ITS for requesting, reviewing, and approving domains and subdomains.

- University Marketing is also proposing the use of Salesforce Marketing Cloud as the preferred platform and only supported tool for mass email marketing communications at NAU. Adoption of this platform will require coordinated governance among several University departments, including University Marketing and ITS. Adopting such a platform would ensure NAU branding is consistent for all outgoing communications, the University owns its data, improved deliverability of emails, and improved ability to ensure compliance with related laws, rules, and regulations.

- ITS Infrastructure & Platform Services is proposing creation of a central repository in NAU’s ServiceNow digital workflow platform allowing multiple users to communicate, collaborate, upload, and distribute applications as a component of Web Advisory governance.

- DMARC authentication improved substantially during the audit as departments learned the benefits of email authentication and worked with third-party application vendors to implement updates to DomainKeys Identified Mail (DKIM) configurations. DKIM is an email authentication method designed to detect forged sender addresses in email or email spoofing, a technique often used in phishing and email spam. (See Exhibit A for additional details).

- Management is aware that an elevated risk exists of exceeding maximum allowable DNS query lookups in the University’s current Sender Policy Framework (SPF) record. SPF is an email authentication method designed to detect forging sender addresses during the delivery of the email. Management is considering subdomain delegation as the preferred email configuration to proactively manage and protect the long-term sustainability of the NAU.EDU domain. Subdomain delegation points internet traffic to the domain / subdomain of a given vendor instead of to NAU.EDU. (See Exhibit A for additional details).

We identified improvement opportunities related to developing NAU.EDU domain and subdomain management governance, including procedures for securing and monitoring University-owned information assets and DNS configuration management, reminding users to actively manage cloud-based accounts, enabling a DMARC oversight approach for all emails originating from the NAU.EDU domain, developing procedures for managing use of third-party mass marketing services, and updating the Vendor Question Form and ITS Checklist to include DMARC management in the vendor onboarding process.

The control standards considered, related control environment assessment and any related improvement opportunities identified are summarized in the following table.
<table>
<thead>
<tr>
<th>General Control Standard</th>
<th>Control Environment/ Assessment</th>
<th>IO No.</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability and Integrity of Financial and Operational Information:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Subdomain naming conventions are standardized to help ensure the reliability of NAU web-based information.</td>
<td><a href="#">Green</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safeguarding of Assets:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Non-NAU.EDU domains are locked, and domain management roles are established to prevent loss and reduce the risk of website hijacking.</td>
<td><a href="#">Green</a></td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>• Domain registrations are routinely reviewed to ensure adequate protection of University-owned assets.</td>
<td><a href="#">Yellow</a></td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>• Processes exist to ensure routine review, modification and/or deletion of records that are key to proper DNS configuration.</td>
<td><a href="#">Yellow</a></td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>• Domains and subdomains are protected by adequately managing and removing abandoned domains.</td>
<td><a href="#">Yellow</a></td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Effectiveness and Efficiency of Operations:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Automated internet domain registration renewals exist to protect against loss of domain registration rights resulting from expiration.</td>
<td><a href="#">Yellow</a></td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>• DMARC enforcement protocols exist to ensure emails originating from the NAU.EDU sending domain are appropriately authenticated.</td>
<td><a href="#">Yellow</a></td>
<td>2</td>
<td>9, 10</td>
</tr>
<tr>
<td>• Mass email communications using Software as a Service (SaaS) platforms are efficiently managed and procured.</td>
<td><a href="#">Yellow</a></td>
<td>3</td>
<td>9, 12</td>
</tr>
<tr>
<td>• Mass email communications using third-party software applications are efficiently managed and procured.</td>
<td><a href="#">Yellow</a></td>
<td>4</td>
<td>9, 16</td>
</tr>
<tr>
<td>• DMARC records are published to inform mail receivers of the disposition expected for messages originating from the NAU.EDU sending domain.</td>
<td><a href="#">Green</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DMARC authentication is monitored for SPF and/or DKIM alignment.</td>
<td><a href="#">Green</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Processes exist to adequately manage SPF records ensuring DNS queries remain within required parameters.</td>
<td><a href="#">Yellow</a></td>
<td>4</td>
<td>9, 16</td>
</tr>
<tr>
<td>• Unique DKIM key pairs are used for each third-party application sending emails on behalf of the NAU.EDU domain.</td>
<td><a href="#">Green</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance with Laws and Regulations:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Outgoing University communications are monitored to help ensure compliance with the CAN-SPAM Act.</td>
<td><a href="#">Yellow</a></td>
<td>3</td>
<td>9, 12</td>
</tr>
<tr>
<td>• Third-party email marketing privacy policies support compliance with the General Data Protection Regulation.</td>
<td><a href="#">Green</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**

- **Reasonably Strong Controls In Place** [Green](#)
- **Opportunity for Improvement** [Yellow](#)
- **Significant Opportunity for Improvement** [Red](#)
We appreciate the assistance and cooperation provided by the staff of Information Technology Services, University Marketing, and various other University departments.

---

Robin Mosness, MS, MS  
Internal Auditor, Sr.  
(928) 523-6459  
robin.mosness@nau.edu

Karletta Jones, CPA, CIA  
Internal Auditor, Sr.  
(928) 523-4136  
karletta.jones@nau.edu

Mark P. Ruppert, CPA, CIA, CISA  
Chief Audit Executive  
(928) 523-6438  
mark.ruppert@nau.edu
Audit Results: Improvement Opportunities & Solutions

1. Creating policies and procedures for managing internet domain assets could improve assurance that:
   - purchased internet domain assets are adequately protected by ensuring domains hosted on University servers are known and recorded,
   - standards for internal and external domain name branding are established, and
   - NAU’s Web presence is better managed and more user-friendly.

SOLUTION: Existing NAU internet domains and subdomains will be reviewed, updated, and properly configured, and inactive domains and subdomains will be removed from the University’s DNS. The University’s domain registrant account will be updated to:
   - Reflect a general ITS procurement card (PCard) as a backup payment method;
   - Ensure NAU contacts are correct;
   - Add backup points of contact, such as administrative and / or billing contacts; and,
   - Set permanent domains to renew automatically.

Responsible Parties:
PJ Way, Director, ITS Infrastructure & Platform Services
Brett West, Assistant Director, ITS Infrastructure & Platform Services
Don Carter, Director, ITS Academic & Research Technology Services
Matthew Wall, Director, University Marketing

Implementation Date: December 31, 2021

DETAILS:

Condition: Analysis of active NAU.EDU internet subdomains and non-NAU.EDU domains noted various challenges as follows:

An internet domain name is a unique name assigned to an entity or person with an established presence on the internet. The name is combined with a generic top-level domain, such as .com, .edu, or .org. Internet subdomains can be created as desired (no required registration) by the domain name owner and are typically reflected as a prefix added to an existing top-level domain name to help the organization and navigation of the related internet presence. Thus, NAU’s top-level domain, NAU.EDU, includes many subdomains, such as IN.NAU.EDU representing NAU’s primary internally facing web presence. Domains and subdomains can be further organized into subdirectories such as IN.NAU.EDU/ITS/ as for the NAU Information Technology Services website.

The University registers and manages the NAU.EDU domain name with EDUCAUSE, the sole internet registrar for names in the .edu domain. The University registers and manages non-NAU.EDU domain names with DomainZoo.com, a domain name registrar.

Non-NAU.EDU domains were originally registered to preserve and protect the NAU brand but have expanded to include domains requested by University departments, employees, and / or external entities. Non-NAU.EDU domain registrations are manually reviewed and renewed by a single NAU employee whose PCard is the sole payment method linked to the registration account.
Testing of active NAU.EDU subdomains and non-NAU.EDU domains disclosed:

a. 199 active NAU.EDU internet subdomains reflected 41 subdomains containing old NAU logos, no NAU logos, broken links, and / or old dates. We were unable to readily determine if these subdomains were being maintained for historical purposes or if they were simply outdated as seemed apparent.

b. 88 non-NAU.EDU domains reflected the following:
   - 14 instances of registered (NAU owned) domains not configured in the NAU DNS,
   - 41 instances of unregistered (may or may not be NAU-owned) domains active in the NAU DNS,
   - 31 instances of domains requiring review and possible removal from the NAU DNS,
   - One instance of a retired NAU employee reported as the current domain registrant of a non-NAU.EDU domain.
   - We also identified that a website hosted by NAU, with the domain registered by a University employee’s Limited Liability Company (LLC), is not included in the University’s DNS and the site appears to be hosted free of charge to an entity funded with federal grants.

Formal policies and procedures for managing NAU’s internet domains and subdomains, including Domain Name System (DNS) configuration, managing domain and / or subdomain requests, and removing inactive domains and / or subdomains, have not been established. Requests have been made informally through email exchanges with ITS staff, resulting in unmanaged NAU domains, subdomains, and / or WordPress sites.

Criteria: Poor DNS configuration management leads to improper updates, slow responses, bad data, potential denial of service, and other problems. National Institutes of Standards and Technology Special Publication 800-81-2 [NIST SP 800-81-2] states, “DNS should have a data repository to store the domain names and their associated IP addresses. Because the number of domain names is large, scalability and performance considerations dictate that it should be distributed. The domain names may even need to be replicated to provide fault tolerance. Second, there should be software that manages this repository and provide the name resolution function. The two functions (managing the domain names repository and providing name resolution service) are provided by the primary DNS component, the name server.”

Cause: Domain name review, approval, monitoring, and management have evolved over many years without establishing policies and procedures to reflect advancements in technologies and practices supporting more effective management of the University’s internet presence.

Effect / Impact: Exposed subdomains can be abused by hackers for phishing and spamming attacks. The user experience can also be negatively impacted by poorly managed and / or structured internet domains and subdomains, resulting in less-than-optimal user experiences when searching for information about NAU and thereby potentially result in the loss of prospective students, donors, and / or other constituents. As such, domain name registration and management create a shared governance opportunity among Information Technology Services, University Marketing, and the NAU Community.
2., 3., & 4.: The remaining improvement opportunities relate to the following summarized information regarding NAU email use and the benefits of applying email authentication protocols.

Beyond day-to-day business communications, NAU processes emails to groups of individuals, both large and small for a variety of purposes, including:

- Marketing to prospective students
- Marketing to or sharing information with existing students
- Soliciting donations either broadly or for specific programs (e.g., athletics, research, etc.)
- Distribution of NAU-wide communications, newsletters, etc.
- Departmental communications, newsletters, etc.
- Communicating with member of online discussion groups

These group communication efforts are most typically handled using third-party services – a.k.a. Software as a Service (SaaS) – and/or third-party software applications, as opposed to using NAU’s daily business email tools (Microsoft Outlook and Google Mail). Such services and/or applications can be obtained and used for free, especially when the email distribution is for low numbers (e.g., 100 or so), or for purchase, such as when supporting mass email communications to multiple hundreds or thousands of individuals. While more than one hundred email services and applications are used by colleges and departments across NAU, there are several key departments involved in the majority of major mass email communication campaigns, including:

- Athletics uses iModules Encompass and MailChimp, both SaaS, and ARMS, a third-party compliance software that includes a communications module for creating and sending mass emails. Enrollment Management uses Salesforce and Salesforce Marketing Cloud, an SaaS.
- NAU Advancement / NAU Foundation uses iModules Encompass and SendGrid, both SaaS.
- Student Affairs uses Emma, a SaaS.

In the best possible scenario, emails sent for the purposes noted above reach the intended recipient email inboxes without being routed by the receiving email server to a spam or junk folder. Without implementing the proper authentication protocols there is much less assurance for the email sender that emails sent reach the intended targets. In particular, Domain-based Message Authentication, Reporting and Conformance (DMARC) protocols help email receivers determine if messages align with what receiving servers know about the origin and legitimacy of the email sender. DMARC and related email authentication protocols are thereby designed to help ensure that receiving servers know the emails are coming from a legitimate organization and allow them to pass through the receiving server spam filters and into the intended email inbox. (See Exhibit A for a more detailed discussion regarding the benefits of and how these authentication protocols work).

NAU uses an email evaluation service called Valimail to determine the email authentication status for emails sent by the various third-party SaaS and applications through the NAU.EDU internet domain. For emails processed for any period of time, Valimail will show the number of
Audit Results: Improvement Opportunities & Solutions

emails processed by an email SaaS or application including identifying emails sent as “Mostly Passing”, Partially Passing”, and “Mostly Failing” DMARC authentication. Passing DMARC indicates the number of emails that were processed using the DMARC protocol and thereby had a much higher probability of passing onto the intended email inboxes; Mostly Failing DMARC indicates the number of emails that were not processed using DMARC and thereby have a much higher probability of being routed to spam or junk folders by the receiving internet servers instead of the intended email inboxes.

For the purposes of the audit analysis and given the magnitude of data to analyze (there are more than 100 third-party email related services / applications used across the NAU Community), we focused our audit efforts on identifying those third-party email SaaS and applications with the highest level of Failed DMARC statistics at the time of our analysis (May 4, 2021), which included the following (see related Valimail report analysis at Exhibit B):

<table>
<thead>
<tr>
<th>THIRD PARTY</th>
<th>TYPE</th>
<th>Emails Processed</th>
<th>Passing DMARC</th>
<th>Failing DMARC</th>
<th>Failure Rate</th>
<th>Related IO#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emma</td>
<td>SaaS</td>
<td>1,395,371</td>
<td>0</td>
<td>1,395,371</td>
<td>100%</td>
<td>3</td>
</tr>
<tr>
<td>SendGrid</td>
<td>SaaS</td>
<td>326,252</td>
<td>7,069</td>
<td>319,183</td>
<td>98%</td>
<td>3</td>
</tr>
<tr>
<td>MailChimp</td>
<td>SaaS</td>
<td>252,082</td>
<td>4,562</td>
<td>247,520</td>
<td>98%</td>
<td>3</td>
</tr>
<tr>
<td>iModules Encompass</td>
<td>Application</td>
<td>1,681,001</td>
<td>54,102</td>
<td>1,626,899</td>
<td>97%</td>
<td>4</td>
</tr>
<tr>
<td>AppArmor</td>
<td>Application</td>
<td>69,827</td>
<td>0</td>
<td>69,827</td>
<td>100%</td>
<td>4</td>
</tr>
<tr>
<td>Salesforce</td>
<td>Application</td>
<td>33,362</td>
<td>0</td>
<td>33,362</td>
<td>100%</td>
<td>4</td>
</tr>
<tr>
<td>TouchNet</td>
<td>Application</td>
<td>32,875</td>
<td>0</td>
<td>32,875</td>
<td>100%</td>
<td>4</td>
</tr>
<tr>
<td>ARMS</td>
<td>Application</td>
<td>6,866</td>
<td>0</td>
<td>6,866</td>
<td>100%</td>
<td>4</td>
</tr>
</tbody>
</table>

The Improvement Opportunities that follow address:
- IO #2: email authentication oversight / monitoring,
- IO #3: control improvements specific to third-party service / SaaS processed emails, and
- IO #4: control improvements specific to emails processed using third-party applications.

2. Establishing and enabling a DMARC oversight and monitoring approach could improve the functioning of University email communications, ensure the validity of authenticated NAU-branded communications, and preserve domain integrity.

SOLUTION: ITS will create a standard to include enabling a DMARC oversight and monitoring policy for all emails sent on behalf of NAU.EDU and non-NAU.EDU domains.

Responsible Parties: Michael Zimmer, Director, ITS ISS
Daniel Wallace, Manager, IT Security Administration, ITS ISS

Implementation Date: December 31, 2021

DETAILS:
Condition: As noted above, during the six months ending May 4, 2021, per Valimail analysis, 112 email services/applications comprising approximately 4.3 million emails sent (32.30% of the
Audit Results: Improvement Opportunities & Solutions

total 13.7 million emails sent during that period), were identified as mostly failing Domain-based Message Authentication, Reporting and Conformance (DMARC), resulting in the likelihood of emails being delivered to spam or junk rather than to intended recipient inboxes. (See Exhibit A for more details on the application of DMARC protocols and Exhibit B for related Valimail report analysis).

DMARC allows domain owners to specify a policy, defined by a parameter “p”, for receivers to handle email messages that fail authentication:

- **p=none** – No enforcement; mail that fails authentication is delivered normally.
- **p=quarantine** – Messages that fail authentication should be quarantined. Usually this means that the messages are delivered to a user’s spam folder.
- **p=reject** – Messages that fail authentication should be discarded, not delivered at all. Some receivers honor this request, while others just mark failing messages as spam.
- In **p=none** mode, domain owners can use the reports sent by mail gateways to examine what messages are being blocked and which IP addresses are sending those messages, allowing domain owners to make changes to SPF and/or DKIM settings to ensure that legitimate messages authenticate.

The NAU.EDU domain currently includes a DMARC policy using Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to determine the authenticity of an email message and protect the domain from unauthorized use. As an organization, NAU’s current DMARC policy is set to be lenient (i.e., p=none) and allow for delivery of all emails, including unauthenticated messages sent by mostly failing services. Mostly failing services include trusted discussion groups, third-party email marketing platforms, and properly vetted and approved third-party software applications. (See Improvement Opportunities 3 and 4 for information regarding email services failing DMARC authentication.)

**Criteria:** Email authentication technologies provide greater assurance on the identity of the sender of a message. Domain-based Message Authentication, Reporting and Conformance (DMARC) helps email receivers determine if messages align with what receivers know about senders. If not, DMARC policies include guidance on how to handle the non-aligned messages. Messages can be authenticated using Sender Policy Framework (SPF) or DomainKeys Identified Mail (DKIM).

The National Institute of Standards and Technology (NIST) Technical Note 1945, Email Authentication Mechanisms: DMARC, SPF and DKIM, states: “DMARC is a component in a compendium of protocols intended to create an open bi-lateral system for authenticating email messages. SPF and DKIM as individual components in that system give message receivers assurance of the authenticity or otherwise of each message from a purported sending domain, but this leaves sending domain owners blind to the effectiveness of their policies posted to the DNS. With DMARC as an additional sending domain policy, also posted in the DNS, receivers can determine sending domain intentions and dispose of messages accordingly and provide feedback on the effects of those policies. Clearly a full deployment of DMARC gives a reporting burden to receivers, who may have to create aggregate reports periodically, sent out to multiple...
Audit Results: Improvement Opportunities & Solutions

sending domain owners, and potentially also send out forensic reports on demand, reporting on spoofed and phishing messages received.”

Further, NIST Technical Note 1945 states, “The usefulness of DMARC to the sending domain is clear: they can receive copious and detailed feedback from a wide spectrum of mail receivers about whether their domain is susceptible to spoofing, quantities of authentic mail delivered, and quantifies of inauthentic mail disposed according to posted DMARC policy. Fine tuning of sender policy can be done, the more that receivers initiate feedback.”

The National Institute of Standards and Technology Special Publication 800-45, [NIST SP 800-45], Version 2 of February 2007, Guidelines on Electronic Mail Security, address the importance of using email authentication practices, including DMARC, SPF, and DKIM for improved email security. NIST SP 800-45, Version 2, states, “Organizations should consider the implementation of cryptographic technologies to protect user authentication and email data. Most standard email protocols default to unencrypted user authentication and send email data in the clear (unencrypted). Sending this data in the clear may allow an attacker to easily compromise a user account and/or intercept and alter unencrypted emails. At minimum, most organizations should encrypt the user authentication session even if they do not encrypt the email data itself. Encrypted user authentication is now supported by most standard and propriety mailbox protocols.”

**Cause:** Email authentication technologies have evolved over the years without establishing policies and procedures to support the University’s expanding email infrastructure.

**Effect / Impact:** The current DMARC policy setting, p=none, provides no message enforcement, thereby increasing the risk that fraudulent messages originating from the NAU.EDU domain are delivered to recipients and that valid emails sent are not delivered to intended recipients’ inboxes.

**SOLUTION:** Recognizing the challenges of managing and monitoring Software as a Service (SaaS) activities given a decentralized user environment and limited resources, ITS and University Marketing management will:

- Create shared messaging to:
  - Remind the campus community of ITS Access Management policies applicable to third-party email marketing accounts and cloud-based social media accounts and applications (i.e., account owners should actively manage accounts and users, update / delete users, and update / delete inactive accounts); Inform the campus community of the benefits of email authentication to improve assurance that all services used, regardless of when and how purchased, are appropriately configured to pass DMARC authentication; and,
Audit Results: Improvement Opportunities & Solutions

- Advise the campus community that implementing proposed DMARC enforcement policies improves assurance that email messages reach intended recipients and offer solutions for authenticating emails;
- Consider alternate mass email marketing solutions for the campus community that enable bulk email communications while meeting University Marketing branding strategies and protecting NAU’s reputation by ensuring all electronic messages are properly authenticated;
- Review the current ITS Checklist and University Software Purchasing Guidelines and update procedures to clearly identify requirements for procurement and use of third-party email marketing platforms, including:
  - Identifying the value to email communications of ensuring such platforms offer solutions for implementing the appropriate email authentication protocols, and
  - Identifying the need to ensure commercially oriented email marketing complies with the CAN-SPAM Act;
- Determine appropriate solutions for authenticating emails of existing third-party marketing providers identified as mostly failing email authentication services; and,
- Offer training to users of email services and applications, as and when necessary.

Responsible Parties:
Steve Burrell, Chief Information Officer, VP, ITS
Harlan Teller, Chief Marketing Officer

Implementation Date: December 31, 2021

DETAILS:
Condition: NAU manages most of its email marketing and recruiting efforts using third-party vendors or services representing Software as a Service (SaaS) platforms. SaaS platforms help automate email distribution services at no cost and / or low cost, depending on the number of email contacts. Many Software as a Service (SaaS) applications exclude the use of technologies allowing receivers to differentiate fraudulent messages from messages properly authenticated to the NAU.EDU domain. Domain-based Message Authentication, Reporting and Conformance (DMARC) protocols provide two options for authenticating email messages: Sender Policy Framework (SPF) and / or DomainKeys Identified Mail (DKIM) - (See Exhibit A for more details on the application of DMARC protocols).

During the six months ending May 4, 2021, per Valimail analysis, 112 email services/applications comprising approximately 4.3 million emails sent (32.30% of the total 13.7 million emails sent during that period), were identified as mostly failing Domain-based Message Authentication, Reporting and Conformance (DMARC), resulting in the likelihood of emails being delivered to spam or junk rather than to intended recipient inboxes. (See Exhibit B for related Valimail report analysis).
Audit Results: Improvement Opportunities & Solutions

The three highest mostly failing services of third-party email marketing service providers (SaaS) at this time were as follows:

<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Emails Processed</th>
<th>Passing DMARC</th>
<th>Failing DMARC</th>
<th>Failure Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emma</td>
<td>1,395,371</td>
<td>0</td>
<td>1,395,371</td>
<td>100%</td>
</tr>
<tr>
<td>SendGrid</td>
<td>326,252</td>
<td>7,069</td>
<td>319,183</td>
<td>98%</td>
</tr>
<tr>
<td>MailChimp</td>
<td>252,082</td>
<td>4,562</td>
<td>247,520</td>
<td>98%</td>
</tr>
</tbody>
</table>

Note: This is an excerpt of the chart included at page 10 representing the SaaS email providers.

Because free SaaS accounts are easily accessible and may be created by multiple unknown / unidentified users, our analyses focused on MailChimp.com users whose PCards were charged for services during FY21 (through April). A review of MailChimp.com accounts reflected the following access management exceptions:

- Four accounts include active user roles for employees no longer affiliated with NAU,
- Four accounts are no longer in use,
- Three accounts last sent NAU communications in 2019,
- One account access is locked, identified as “Protected by Authenticator”, and,
- MailChimp account access includes two-factor authentication requiring user email accounts; however, one account role was created using a non-NAU.EDU email address, thereby negating the two-factor authentication protection for that account.

Charges for third-party email marketing services are incurred at the time of service and without clear policy guidance for proper treatment of ITS pre-approval requirements, in that procurements handled through a purchase requisition are flagged for proper ITS pre-approval review, but procurements handled using a PCard are not easily flagged. A review of FY21 PCard charges through April 2021 reflected 23 departments incurred charges for third-party marketing services from four different SaaS providers, including Emma, MailChimp, SendGrid and Smore.com.

ITS procedures require review and approval of all University software purchases, including hosted cloud-based software. When completing purchases using a purchasing requisition instead of a PCard, completing an ITS Checklist and NAUVAT form is required. Completing the ITS Checklist and NAUVAT forms may be applicable for primary University-wide accounts on a per-vendor basis; however, departments who separately pursue services or applications from the same vendor already used by another department have been required to request completion of the same checklist and form, even though NAU has already received such information from the vendor. As such, requiring each department / user to comply with procedures for the same vendor creates inefficiencies in the process. Current Comptroller policies prohibit the purchase of software, resulting in Notice of Violations issued to PCard users who procure third-party marketing services.

The FY21 ITS Checklist status report and purchases inventory reflect that two departments completed the required ITS Checklist procuring third-party marketing services prior to utilizing those services and 21 departments procured such services without completing the ITS Checklist. However, all departments interviewed believed they are authorized to engage in the communication activities.
Audit Results: Improvement Opportunities & Solutions

Finally, without a formal review process for email marketing campaigns outside of the Marketing Department, NAU cannot be assured that such communications comply with applicable provisions of the Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act, which sets forth basic principles for differentiating legal and illegal commercially oriented email. Note that we did not test NAU email marketing campaigns for specific compliance elements; however, we are noting the need for an internal review process that ensures such compliance on an ongoing basis.

Criteria: Email authentication technologies provide greater assurance on the identity of the sender of a message, which improves deliverability and security. Domain-based Message Authentication, Reporting and Conformance (DMARC) protocols help email receivers determine if messages align with what receivers know about senders. If not, DMARC policies include guidance on how to handle the non-aligned messages. Messages can be authenticated using Sender Policy Framework (SPF) or DomainKeys Identified Mail (DKIM). (See Exhibit A for more details on DMARC authentication policies).

The ITS Purchasing, Licensing, and Using Technology at NAU procedures require review and approval by the Accessibility Office and by Contracts, Purchasing, and Risk Management (CPRM) prior to the purchase of hardware and / or software, including hosted cloud-based software. The requirements currently include providing vendor accessibility documentation and a Northern Arizona University Vendor Assessment Tool (NAUVAT) if the software is vendor hosted or cloud based, regardless of whether the purchase is completed through a purchase requisition or a PCard. Optional documentation may include the Vendor Request Form and the ITS Checklist, which require detailed ITS information from the vendor. (See Improvement Opportunity 3 for improvement opportunities related to these forms).

NAU Comptroller Policy CMP 401-03, Prohibited Transactions, states, “All software purchases must be approved, prior to purchase, by Information Technology Services and NAU’s Accessibility Team. If you are looking to purchase software that is not part of the university's Software Support policy, please review Information Technologies Services “University Software Purchasing Guidelines” on their Software support page under “Purchasing Software” before making any purchases. You will also need to complete the Accessibility Approvals/Exceptions form.”

The National Institute of Standards and Technology Special Publication 800-45, [NIST SP 800-45], Version 2 of February 2007, Guidelines on Electronic Mail Security (see additional details for this criteria reference at IO 2, Criteria).

The Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003 sets forth the basic legal principles that differentiate legal and illegal commercially oriented email. See 15 U.S.C. § 7704(a). According to these principles, the senders of commercially oriented email will be engaging in legal activity, so long as:

- The header of the commercial email (indicating the sending source, destination, and routing information) doesn't contain materially false or materially misleading information;
- The subject line doesn't contain deceptive information;
Audit Results: Improvement Opportunities & Solutions

- The email provides "clear and conspicuous" identification that it is an advertisement or solicitation;
- The email includes some type of return email address, which can be used to indicate that the recipient no longer wishes to receive spam email from the sender (i.e., to "opt-out");
- The email contains "clear and conspicuous" notice of the opportunity to opt-out of receiving future emails from the sender;
- The email has not been sent after the sender received notice that the recipient no longer wishes to receive email from the sender (i.e., has "opted-out"); and
- The email contains a valid, physical postal address for the sender.\(^1\)

Cause: University Marketing made a previous attempt at establishing a University-wide solution for creating, approving, and sending mass email communications to constituents using MailChimp.com, but it was unsuccessful due to the inability to truly enforce use given the prevalence of free services and ease of purchase by many members of the NAU Community. While current ITS procedures require completion of certain forms and checklists (see IO #4) and review by IT staff prior to purchase, this process is not easily applied to PCard purchases. An individual can use a PCard to make a direct purchase from a vendor without going through the Purchasing Department, which flags IT-related purchases for completion of the applicable forms and checklists.

Effect / Impact: Undefined and / or inconsistent policies and procedures create confusion and / or can lead to non-compliance of established procedures. Unauthenticated messages can create reputation and IT security risk, and / or result in decreased return on investment. Compliance with related laws, rules and regulations may also be undermined without a formal process and embedded reviews to ensure proper compliance.

4. Updating the ITS Vendor Question Form and ITS Checklist to include third-party vendor email configuration assessment could help preserve domain integrity by monitoring to help ensure that email services use authentication protocols.

SOLUTION: The ITS Infrastructure & Platform Services Core Systems Team and the ITS Information Security Services Security Operations Center (ISS SOC) Team are working with University departments whose vendors experience mostly failing services to authenticate NAU.EDU emails. The ITS Strategic Planning, Implementation & Education Services (SPIES) Solutions Architecture Team will update the Vendor Question Form and ITS Checklist to include consideration of third-party vendor email configuration, ensuring emails are properly authenticated prior to application implementation. The Vendor Question Form and ITS Checklist will include identifying if the vendor will send email as representing NAU. If so, the vendor should send emails authenticated by Sender Policy Framework (SPF) and / or DomainKeys Identified

\(^1\) Source: Cornell Law School, Legal Information Institute: https://www.law.cornell.edu/wex/inbox/can-spam_act_core_requirements
Audit Results: Improvement Opportunities & Solutions

Mail (DKIM). As a best practice, subdomain delegation will be pursued where possible to implement email authentication. Subdomain delegation points internet traffic to the domain/subdomain of a given vendor instead of to NAU.EDU.

Responsible Parties:
PJ Way, Director, ITS Infrastructure & Platform Services
Brett West, Assistant Director, ITS Infrastructure & Platform Services
Andrea Stalker, Director, ITS SPIES
Michael Zimmer, Director, ITS ISS
Daniel Wallace, Manager, IT Security Administration, ITS ISS

Implementation Date:
December 31, 2021

DETAILS:
Condition: Many properly vetted and approved software applications exclude the use of technologies allowing receivers to differentiate fraudulent messages from messages properly authenticated to the NAU.EDU domain. While applications properly vetted through the NAU procurement process include completion of the required Vendor Questionnaire and IT Security Checklist forms, email configuration is not considered since the current forms do not include assessing vendor email functionality and vendor ability to support DMARC email authentication protocols.

During the six months ending May 4, 2021, per Valimail analysis, 112 email services/applications comprising approximately 4.3 million emails sent (32.30% of the total 13.7 million emails sent during that period), were identified as mostly failing Domain-based Message Authentication, Reporting and Conformance (DMARC), resulting in the likelihood of emails being delivered to spam or junk rather than to intended recipient inboxes. (See Exhibit A for more details on the application of DMARC protocols).

The five highest mostly failing services of approved third-party software applications at this time were as follows:

<table>
<thead>
<tr>
<th>Application</th>
<th>Emails Processed</th>
<th>Passing DMARC</th>
<th>Failing DMARC</th>
<th>Failure Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>iModules Encompass</td>
<td>1,681,001</td>
<td>54,102</td>
<td>1,626,899</td>
<td>97%</td>
</tr>
<tr>
<td>AppArmor</td>
<td>69,827</td>
<td>0</td>
<td>69,827</td>
<td>100%</td>
</tr>
<tr>
<td>Salesforce</td>
<td>33,362</td>
<td>0</td>
<td>33,362</td>
<td>100%</td>
</tr>
<tr>
<td>TouchNet</td>
<td>32,875</td>
<td>0</td>
<td>32,875</td>
<td>100%</td>
</tr>
<tr>
<td>ARMS</td>
<td>6,866</td>
<td>0</td>
<td>6,866</td>
<td>100%</td>
</tr>
</tbody>
</table>

Note: This is an excerpt of the chart included at page 10 representing the email applications.

Criteria: Email authentication technologies provide greater assurance on the identity of the sender of a message, which improves deliverability and security. Domain-based Message Authentication, Reporting and Conformance (DMARC) protocols help email receivers determine if messages align with what receivers know about senders. If not, DMARC policies include guidance on how to handle the non-aligned messages. Messages can be authenticated using...
Audit Results: Improvement Opportunities & Solutions

Sender Policy Framework (SPF) or DomainKeys Identified Mail (DKIM). (See Exhibit A for more details on the email authentication).

The National Institute of Standards and Technology Special Publication 800-45, [NIST SP 800-45], Version 2 of February 2007, Guidelines on Electronic Mail Security (see additional details for this criteria reference at IO 2, Criteria).

**Cause:** Email authentication technologies have evolved over the years without establishing policies and procedures to support the University’s expanding email infrastructure.

**Effect / Impact:** NAU purchases and uses third-party applications that send unauthenticated emails, resulting in wasted time and financial resources while increasing the potential for IT security issues.
Email has been a core application of computer networking since early development and adoption of the Internet. The core protocol adopted in 1982, Simple Mail Transport Protocol (SMTP), is still operated today; however, it is more susceptible to a wide range of attacks, especially, and more recently within higher education environments.

While most users assume that a sent email will reach its intended recipient, email services are more complex than they appear. Emails are processed by a sending server as well as a receiving server. Certain automated protocols must be in place to help the receiving server confirm the email sent is from a legitimate source. Without such authentication protocols, a sent email may be delivered to a recipient’s spam or junk folder rather than the recipient’s inbox, which means mass email marketing efforts to prospective students, donors, and other constituents is significantly compromised.

The primary protocol supporting email authentication is known as Domain-based Message Authentication, Reporting and Conformance (DMARC). Applying DMARC enforcement policies, using the internet standards Sender Policy Framework (SPF) and / or DomainKeys Identified Mail (DKIM), provides validation to ensure recipients that the email communications received from the NAU.EDU sending domain are official and authenticated. Without such authentication, NAU has no assurance that recipient email servers will allow those emails to pass to the intended recipient.

Sender Policy Framework (SPF) is used to authenticate the sender of an email. With an SPF record in place, Internet Service Providers can verify that a mail server is authorized to send email for a specific domain. An SPF record is a Domain Name System (DNS) TXT record containing a list of the Internet Protocol (IP) addresses that are allowed to send email on behalf of the NAU.EDU domain. To fully resolve an SPF record, specifications limit the number of DNS lookups to ten and no more than 255 characters in the string.

DomainKeys Identified Mail (DKIM) is also used to authenticate the sender of an email by cryptographically signing each outgoing email message linked to the NAU.EDU domain. The recipient system can verify the signature by looking up the public key published in the domain name system (DNS). A valid signature also assures the recipient that parts of the email have not been modified since the signature was affixed.

According to the National Institute of Standards and Technology (NIST), “Domain-based Message Authentication, Reporting and Conformance (DMARC) was conceived to allow email senders to specify policy on how their email should be handled, the types of security report that receivers can send back, and the frequency of sending those reports. Standardized handling of SPF and DKIM removes the guesswork about whether a given message is authentic, benefitting receivers by allowing more certainty in quarantining and rejecting unauthorized mail. In particular, receivers compare the “From” address in the message to the SPF and DKIM results, if present, and the DMARC policy in the DNS. The results are used to determine how the mail should be handled. The receiver sends reports to the domain owner about mail claiming to originate from their domain. These reports should illuminate the extent to which unauthorized users are using the domain, and the proportion of mail received that is ‘good’.”

---

2 NIST SP 800-177, Trustworthy Email, http://dx.doi.org/10.6028/NIST.SP.800-177, accessed May 2021.
EXHIBIT A – Background Information: Email Authentication
(Page 2 of 2)

The image below illustrates the relationship between sending and receiving mail servers and the DMARC policy validation process:
As shown in the image below for the six-month period ending May 4, 2021, approximately 13.7 million emails were sent on behalf of the "@NAU.EDU" domain or subdomains. Of those emails, approximately 4.3 million (32.30%) were unverifiable by the recipients, increasing the likelihood of emails being redirected to junk mailboxes, potentially costing the University in recruitment, engagement, and/or email reputation.

---

The distribution of success and failure is further broken down by services, as follows, and as presented in the subsequent image:

- **“Mostly Passing” services** – the vast majority of messages sent by services in this category are properly authenticated
- **“Partially Passing” services** – messages sent by services in this category have a mix of authenticated and unauthenticated messages
- **“Mostly Failing” services** – the majority of messages sent by services in this category are not authenticated and will not be delivered to the inbox when DMARC is enabled.

### DMARC Authentication Test Details

<table>
<thead>
<tr>
<th>DMARC Authentication</th>
<th>Mostly Passing 8 Services</th>
<th>Mostly Failing 112 Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>13,701,414</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9,354,943</td>
<td>68.28%</td>
<td></td>
</tr>
<tr>
<td>with DKIM</td>
<td>43.98%</td>
<td></td>
</tr>
<tr>
<td>6,025,772</td>
<td></td>
<td></td>
</tr>
<tr>
<td>with SPF</td>
<td>65.43%</td>
<td></td>
</tr>
<tr>
<td>8,964,626</td>
<td></td>
<td></td>
</tr>
<tr>
<td>with DMARC override</td>
<td>0.40%</td>
<td></td>
</tr>
<tr>
<td>55,277</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failing</td>
<td>4,346,471</td>
<td></td>
</tr>
<tr>
<td>31.72%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Salesforce Marketing Cloud**
  - Pass: 4,899,516 (99.62%)
  - Fail: 23,478 (0.48%)
- **Microsoft Office 365**
  - Pass: 1,011,406 (97.94%)
  - Fail: 21,282 (2.06%)
- **Google Workspace**
  - Pass: 1,850,008 (99.92%)
  - Fail: 152 (0.08%)
- **Marketeto**

### Unidentified Senders

- **20.1% of total**

<table>
<thead>
<tr>
<th>Passing DMARC</th>
<th>2,353,311</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failing DMARC</td>
<td>406,916</td>
</tr>
</tbody>
</table>

### Internal Sources

- **5.4% of total**

<table>
<thead>
<tr>
<th>Passing DMARC</th>
<th>708,892</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failing DMARC</td>
<td>30,400</td>
</tr>
</tbody>
</table>

### Partially Passing 5 Services

<table>
<thead>
<tr>
<th>Qualtrics</th>
<th>14,640</th>
</tr>
</thead>
<tbody>
<tr>
<td>(82.82%)</td>
<td></td>
</tr>
<tr>
<td>Fail: 3,037</td>
<td>(17.18%)</td>
</tr>
<tr>
<td>Blackbaud Award Management</td>
<td>156</td>
</tr>
<tr>
<td>Pass: 1,011,406</td>
<td>(97.94%)</td>
</tr>
<tr>
<td>Fail: 21,282</td>
<td>(2.06%)</td>
</tr>
<tr>
<td>MarchingOrder</td>
<td>131</td>
</tr>
<tr>
<td>Pass: 131</td>
<td>(97.92%)</td>
</tr>
<tr>
<td>Fail: 18</td>
<td>(12.08%)</td>
</tr>
<tr>
<td>Constant Contact</td>
<td>120</td>
</tr>
<tr>
<td>Pass: 120</td>
<td>(97.92%)</td>
</tr>
</tbody>
</table>

### Mostly Failing 112 Services

<table>
<thead>
<tr>
<th>Emma</th>
<th>112 Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass: 0</td>
<td>(0.00%)</td>
</tr>
<tr>
<td>Fail: 1,423,833</td>
<td>(100.00%)</td>
</tr>
<tr>
<td>SendGrid</td>
<td>7,831</td>
</tr>
<tr>
<td>Pass: 7,831</td>
<td>(2.39%)</td>
</tr>
<tr>
<td>Fail: 319,183</td>
<td>(97.61%)</td>
</tr>
<tr>
<td>MailChimp</td>
<td>4,592</td>
</tr>
<tr>
<td>Pass: 4,592</td>
<td>(1.79%)</td>
</tr>
<tr>
<td>Fail: 251,640</td>
<td>(98.21%)</td>
</tr>
</tbody>
</table>
Testing included identifying the 17 highest mostly failing email services by type: discussion boards / email discussion groups, third-party marketing platforms, and third-party software applications. Working with NAU departments and their vendor support teams, we requested Canonical Name (CNAME) records, added those records to the domain name system (DNS), confirmed with vendors that records were published, and monitored DKIM alignment to ensure messages passed DMARC. The following images reflect DMARC status for three mostly failing third-party software applications email services before and after DKIM configuration. The bar charts below identify email messages failing DMARC authentication in red in early to mid-June and then passing DMARC authentication (following implementation of the applicable email authentication protocols) in blue through mid to late June for the iModules Compass, Salesforce, and Arms third-party email services.

**iModules Encompass**

![Graph showing DMARC status for iModules Encompass from 06/01/2021 to 06/27/2021]

**Salesforce**

![Graph showing DMARC status for Salesforce from 06/01/2021 to 06/27/2021]

**ARMS**

![Graph showing DMARC status for ARMS from 06/01/2021 to 06/27/2021]