Future-proofing email relay for federal agencies

As system-generated email continues to rise, federal email systems require new approaches. But legacy relay systems are holding them back.

proofpoint.

Email relay may be invisible to most users, but it is foundational to how federal agencies deliver services and maintain public trust. For decades, email inside federal agencies followed a predictable pattern: human users sent messages; applications sent limited, rules-based notifications; and on-premises relay systems quietly supported delivery.

Today, federal agencies send millions of system-generated emails every day — from eligibility notices to appointment reminders and security alerts — and an increasing share of those messages are triggered by automation and AI-enabled tools. These messages are not peripheral to mission delivery; they are mission delivery. When they fail or behave unexpectedly, the impact is immediate and tangible: citizens miss appointments, benefits get delayed and confidence in government communications erodes.

Yet while the role of email has expanded, much of the infrastructure that supports system-generated messages has not. Many agencies still rely on legacy relay platforms that are designed for static applications, predictable volumes and tightly controlled on-premises environments. As agencies introduce AI agents and automated decision systems, the gap between how email is used today and how it is governed continues to widen. That gap increases operational risk at precisely the moment agencies can least afford it.

The evolving role of federal email

Email inside federal agencies is no longer primarily user-driven. It is system-driven — and increasingly AI-driven. Applications, SaaS platforms and automated agents now communicate directly with citizens, partners and employees at scale, often without a human in the loop.

As agencies digitize services, system-generated emails have become a primary delivery mechanism for mission outcomes.

Cloud adoption and automation have accelerated this shift, moving user email to modern platforms while dramatically increasing the number of backend systems that rely on email to function. AI-enabled tools further change the risk profile. Unlike traditional applications that send fixed, pre-approved messages, AI agents can generate content dynamically, react to data in real time and, if improperly governed, behave in unexpected ways.

The result is a split model. Modern cloud email is used for users, meanwhile aging infrastructure supports system-generated messages. That disconnect increases complexity and risk at the very moment email has become more central to mission delivery.

“Some agencies have been limping along using their on-premises infrastructure,” said Craig Temple, product marketing manager at Proofpoint. “But they’re facing end-of-life or end-of-support for some platforms, and agencies do have to do something about it.”

The hidden risks of legacy relay infrastructure

Many legacy email relay systems were built for a time when a small, well-defined set of applications sent predictable, pre-approved messages. Traditional systems like invoicing or case management applications transmitted a fixed set of known fields, making it easier to inspect, control and secure data in motion.

That assumption no longer holds. Today, agencies rely on dozens — sometimes hundreds — of applications, SaaS platforms and increasingly AI-enabled agents to communicate directly with citizens, partners and employees. With AI agents, application traffic shifts from being bounded and predictable to dynamic and open-ended, materially increasing both security and data leakage risk.

Legacy relays typically offer limited visibility into which systems are sending on an agency's behalf, how content is generated or what data is included in outbound messages. As agencies introduce AI agents that generate email autonomously based on prompts, context and learned behavior, that lack of visibility becomes more consequential. These systems are not inherently constrained to a defined dataset. As a result, there's an increased likelihood that sensitive, proprietary or regulated information may be inadvertently included in outbound communications.

"Organizations may not know all the different applications or sources that are sending on their behalf," Temple said. "It creates a lot of vulnerability."

As agent-driven activity scales, even small prompt or context errors can propagate widely. What would have been a contained mistake in a conventional application can quickly become a systemic exposure event — replicated across thousands or millions of messages before it is detected. In that environment, relying on legacy relay controls or assuming correct agent behavior is no longer sufficient.

Meanwhile, the external email ecosystem is tightening standards. Major inbox providers now require strong sender authentication, including DKIM signing and DMARC alignment. Systems that cannot meet these requirements risk having messages delayed, filtered or rejected altogether.

For agencies such as the Department of Health and Human Services or the Department of Veterans Affairs, these failures are not abstract. Email is a primary channel for confirming appointments, notifying beneficiaries about eligibility and delivering time-sensitive health and service updates. When messages do not arrive — or are flagged as suspicious — citizens lose access to critical, life-saving service.

A purpose-built path to modernization

Modernizing requires more than replacing aging servers. It requires a new approach to how system-generated email is governed, secured and delivered.

Proofpoint Federal Email Relay (FER) is designed specifically for this purpose.

"FER authenticates every sending source," Temple said. Only verified applications and systems can relay messages. This helps prevent impersonation and ensures each communication originates from a trusted entity.

Once the message enters the relay, FER applies antivirus and anti-spam scanning. It also offers optional data loss prevention for sensitive information, such as PII and PHI. And it DKIM-signs all outbound email to support DMARC compliance and message integrity.

In practice, this means agencies can deliver system-generated messages with confidence — a feature Temple said is particularly critical for high-volume communications from agencies where delayed or rejected messages can disrupt services, confuse beneficiaries and undermine public trust.

Critically, FER operates in a dedicated environment, separate from user email. High-volume system traffic does not interfere with day-to-day communications or disrupt agency operations. “All of the controls that we have in place for user-generated emails are the same ones we use for application-generated traffic,” said Temple. “We do it in a separate, secure environment.”

Proofpoint’s cloud-based architecture also removes the operational burden of maintaining on-premises infrastructure. Agencies can scale securely as volumes increase — whether from expanded citizen services, automation or emerging AI-driven systems — without managing hardware or capacity planning.

“FER is more than a relay,” Temple said. It’s a “security-first, mission-focused” platform that ensures system-generated emails are authenticated, protected and reliable.

Security and operational controls are built in:

- **Dedicated relay environment**
- **Authenticated sending sources**
- **DKIM signing and DMARC alignment**
- **Antivirus and anti-spam scanning**

Click to Learn more about how Proofpoint is helping federal agencies modernize email relays.