# *Modernizing and Securing U.S. Government Networks*

**Advances in Network Resilience from Internet Protocol-Based Networks**

*by Clete Johnson and Evelyn Remaley*[1]
*August 2026*

## Executive Summary

Speed, capacity, reliability, and security are key measures of communications network functionality. Across all these measures, modern fiber and wireless networks built on Internet Protocol (IP) "packet switching" and next generation technologies far outperform networks built on Time-Division Multiplexing (TDM)-based technology. Transitioning to IP-based and related advanced network capabilities[2] is not simply an IT modernization preference; it is a mission assurance imperative.

Scalability and survivability distinguish IP-based networks from TDM-based networks. TDM-based networks were designed with a single primary function in mind – voice calls – and were not designed to meet the demands of today's complex and dynamic service, mobility, and security environment. From a physical standpoint, copper-based TDM networks are also more susceptible to water damage and are increasingly targeted by thieves, leading to recurrent outages. When outages occur, it takes longer to repair TDM-based networks because today's supply chain and workforce no longer reflect a market where TDM is in demand. In short, the parts and people to keep these networks running are often unavailable.

IP-based networks, on the other hand, were designed for resilience. Whereas TDM networks send communications along a designated switched circuit, IP networks break communications down into small packets that are separated and routed for speed and survivability across a range of distributed paths and nodes and then reassembled at the end destination allowing for multiple possible data routes. Think of the data packets as a set of siblings coming home for the holidays from various locations and via various routes. No matter the disruptions and reroutes, all of them make it home. The modular, dynamic, and interoperable nature of IP networks also make them easy and quick to scale for evolving network and data needs. The early developers of the TCP/IP protocol meant to enable different communications modalities – radio communications, terrestrial, even satellite – to speak one digital language. In response, IP-based communications have proven remarkably resilient, surviving a wide range of logical and physical disruptions.

At the individual level, the student, worker, or business owner on an IP-based connection will be better off than their counterpart on a TDM-based connection. IP-based consumers can communicate in multiple ways, engage in extraordinarily data-intensive tasks, and do so more quickly and more securely than on TDM-based networks. This same principle applies at a larger

---

[1] The Liberty Bell Project is a 501(c)(3) non-profit education and training organization that aims to strengthen the infrastructure of our free society; the organization does not conduct advocacy of any kind. The authors' opinions derive from decades of experience in senior roles in the U.S. government and the private sector communications industry.

[2] IP-based networks can run over wireless access networks such as 4G LTE and 5G as well as over wired infrastructure, including Ethernet switching, DWDM optical transport, and dark fiber, which can also carry non-IP traffic. For brevity, this paper uses the term "IP-based networks" as shorthand for all these elements of advanced and next generation networking.

scale as well — a government agency relying on an IP-based network will be better off from both an operational and security perspective than an agency relying on TDM-based networks.

Despite this reality, for a variety of reasons, many federal agencies across the U.S. government (USG) still rely on TDM-based networks. This reliance on legacy technology for modern demands presents challenges that are deeper than inconvenience or budget shortfalls. Indeed, continued reliance on TDM networks raises continuity and security liabilities that put critical USG missions and communications at risk. Further, it places the USG behind in embracing the functional benefits of IP networking, which is the foundation for next generation and AI enhanced network functionalities. Through numerous executive actions and orders, the Administration has called on agencies to rapidly transition to modernized networks to ensure the highest level of security, *and* to have an early seat at the table in shaping advanced IOT, robotics, mobility, sensing, and smart infrastructure – all of which build on IP interoperability.

Many TDM-based systems are decades old, with equipment and components nearing the end of their lifespans and replacements often no longer in production. When parts break, the impact goes beyond limiting operational capacity and efficiency — it potentially creates a security vulnerability that bad actors can exploit to attack government wide systems and operations.

Even when all parts are working, TDM networks have limitations in their security capabilities as compared to IP networks, leaving agencies at a dangerous disadvantage when defending against increasing cybersecurity threats. IP networks support end-to-end encryption, dynamic threat monitoring, and advanced authentication. Basic TDM security rests on its closed, physical nature, and separated control plane, but TDM cannot support many software-based cybersecurity tools that protect modern data and voice infrastructure. Not only are TDM networks slower and less capable than IP networks, but they are extremely limited in the comparative security features they can offer and the frameworks they can adopt.

Cutting-edge, advanced and large-scale Artificial Intelligence (AI) models — often referred to as "frontier AI" — have resulted in new and increasingly sophisticated cyber-attacks emerging at a blistering pace, raising the cyber risk for TDM network architectures drastically. The USG must address these legacy risks with urgency in order to secure its critical networks. Federal agencies need to expeditiously transition from TDM to IP-based networks that are supported by assured supply chains and allow for enhanced security capabilities. The Department of Homeland Security (DHS) and the Federal Aviation Administration (FAA) have already begun to modernize their communications infrastructure giving other USG agencies a path to follow.

Agencies need top-down guidance to facilitate progress. The Administration has a strong case with Congress for adequate resources for these projects and should also work with industry to lower regulatory hurdles and prepare a host of IP-based solutions. The Cybersecurity and Infrastructure Security Agency (CISA) has ordered civilian agencies to identify and retire End-of-Support (EOS) edge devices;[3] this is a necessary step for the broader transition to advanced network technology that can support security functionality necessary to address today's threats.

[3] Cybersecurity and Infrastructure Security Agency, *Binding Operational Directive 26-02: Mitigating Risk From End-of-Support Edge Devices* (Feb. 5, 2026), https://www.cisa.gov/news-events/directives/bod-26-02-mitigating-risk-end-support-edge-devices.

**Illustrative Threat Scenario: Hypothetical Arctic Communications Security Threat**

Government agencies need to be able to depend on secure, resilient communications network infrastructure to exchange information quickly and securely, as well as employ applications that increase efficiency and effectiveness. TDM-based networks simply cannot provide that foundation in many cases. Consider the following hypothetical threat scenario that demonstrates the limitations of TDM-based networks.[4]

With new shipping lanes opening and untapped oil, natural gas, and rare earth minerals available in the Arctic, the region is growing in strategic importance for the United States, as well as for China and Russia. China has increased its trade presence through its "Polar Silk Road" initiative, and Russia has expanded its military bases and fleet in the region.

The United States also has installations like Pituffik Space Base in Greenland and the North Warning System (NWS), jointly operated with Canada, consisting of 47 radar sites across northern Alaska and Canada that detect aircraft and provide a real-time aerial picture of the Arctic region. Fast, reliable, and secure communications at these U.S. installations and all others across the region are critical to national security. However, many U.S. installations – including Pituffik Space Base and NWS radar stations – rely on TDM-based equipment that was installed decades ago.

In this hypothetical but plausible scenario, Russia is engaging in ramped-up military exercises near Alaska. NWS radar sites are on high-alert, and certain TDM-based network segments are becoming strained. Eventually, a TDM multiplexer at a radar site in Alaska fails under the heavy load. After two decades of running continuously in one of the harshest environments in the world, the equipment has met its limit.

Operators scramble to find a replacement multiplexer, but the original equipment manufacturer (OEM) ceased production of the component years ago. Even if a replacement is found, delivering it would take at least 72 hours. As a result, the radar site goes partially dark, creating a significant surveillance gap. At the same time, sophisticated Russian cyber operators who routinely study U.S. communications patterns see a vulnerability. They target TDM systems running on software that is publicly documented as vulnerable. These systems, without "zero-trust architecture," real-time threat detection, and other cyber defense capabilities, are vulnerable to Russian exploitation even without reliance on the capabilities of the advanced "frontier AI" models being released today.

Russian cyber operators introduce subtle changes to compromise other NWS radar sites and TDM-circuits at Pituffik Space Base. This creates further surveillance gaps and begins to degrade the quality and security of voice communications between Pituffik and other installations. In just a few hours, U.S. communications and security across the region is severely compromised. The recovery timeline is not hours but days. Russian networks, on the other hand,

[4] Authors' Note: This is a hypothetical scenario constructed for illustrative purposes. It is based on publicly available information regarding the Defense Information Systems Agency (DISA), the Defense Information Systems Network (DISN), U.S. military infrastructure in the Arctic, and well-established challenges associated with legacy TDM infrastructure. Real organizations, locations, and strategic dynamics are referenced to provide context, but this scenario does not describe any actual event or confirmed incident.

remain impervious to the impacts of the harsh Arctic environment, functioning on the highly resilient components of a modernized, IP-based infrastructure.

**U.S. Security and Resilience Must Account for AI Advances that TDM Networks Cannot**

As the hypothetical Arctic threat scenario illustrates, TDM-based communications infrastructure puts the U.S. at a technological disadvantage relative to IP networks. This legacy architecture generates sustained and persistent national security risk, even when a readily available advanced alternative exists. The USG remains one of the largest users of TDM-based technologies in the world, despite service providers transitioning to IP networks leveraging fiber, 5G wireless, and Low Earth Orbit (LEO) satellite. While the Arctic hypothetical above applies to Department of War (DoW) networks, other departments and agencies across the USG are vulnerable to their own attacks and failures.

The reliance also exists at state and local government levels and across critical industries. For example, Public Safety Answering Points (PSAPs) — the 911 call centers that facilitate response to emergencies — are required to transition away from TDM-based connections to more modern networks, but many are still connected to TDM-based lines and other equipment that is ill-suited support secure, resilient public safety communications. Likewise, energy grids and hospitals rely on outdated TDM-based technology with huge operational and security vulnerabilities.

One major issue for TDM networks is that in many cases, parts in use today have been running since the 1990s and are reaching the end of their lifespan. OEMs have also stopped producing certain parts, so when replacements are needed, operators must turn to the resale market. This presents its own security concerns, as it is difficult to track the origin of resale equipment and verify whether it meets security standards. Even if a replacement is found, many skilled TDM-based technicians have retired. What this means is that, over time, the ability to recover from equipment failures will only become more difficult, costly and time-consuming.

But more important than the supply chain vulnerability considerations is the new era of AI-driven dynamic threats that we have just entered.  Fortunately, IP-based networks are architected to adapt and upgrade in real time to defend against dynamic cyber threats.

**The advanced cybersecurity capabilities of frontier AI models have significantly increased the urgency to transition to IP-based infrastructure.** Advanced "frontier"  AI models have raised the threat level of reliance on TDM network architectures drastically, resulting in new and increasingly sophisticated cyber attacks emerging at a blistering pace that TDM networks do not have the agility to defend against. We are now at a critical inflection point for replacing these legacy systems and their unsupported and difficult-to-patch core architectures with IP-based networks. Although in the past agencies were able to raise viable arguments for extending the transition timeline, that window has passed. No matter the function the network supports, if it is not IP-based, it is too vulnerable and can present risk across the broader enterprise.

Some networks in the past were deemed "less critical" and therefore placed on low priority for the transition to IP, but in the current threat environment those decisions should be revisited as sensing and other network functions are likely now more affordable on an IP system, offering better or more targeted functionality and greater security assurance. Although agencies may see extending the transition timeline to be a cost-limiting move, long term costs skyrocket as legacy equipment becomes more and more expensive — and in some cases impossible — to repair and replace over time, leading to further delays or disruption. Putting off upgrades, even for "less critical" networks, will also become riskier as frontier AI models can patch together multiple minor vulnerabilities to create major vulnerabilities that would have been difficult to identify previously.

As frontier AI models such as Mythos 5 and GPT 5.5 emerge with advanced vulnerability detection capabilities, it is essential that the ecosystem transition to IP networks that are conducive to efficient and rapid patching and repairs. Federal agencies, especially those undertaking national security and essential functions, must ensure that the networks they rely on are designed to enable patching and mitigation, particularly in this rapid-fire environment of AI-enhanced cyber capabilities.

Federal agencies have known of the need to transition to IP-enabled networks for decades. Although TDM networks were reliable for their era, IP networks offer unrivaled resiliency in their ability to reroute, self-repair and survive, and most of all to upgrade and mitigate when vulnerabilities are discovered.

With the TDM ecosystem generally being at end of life, federal agencies are running out of time for executing this transition. As federal contracts are being planned and designed for the AI era, it is critical that the transition to IP for all remaining legacy networks is built into the planning and budgeting process today. The USG can no longer afford to have sensor networks, air traffic controllers, defense bases, radar detectors, or other essential government services reliant on 20th century network architecture that cannot accommodate dynamic security measures. Today's sophisticated adversaries are ready to use any weak link in the federal ecosystem as a path to disrupting our most essential assets — U.S. critical infrastructure.

To protect our nation from this threat, we must act with urgency. The Trump Administration has recognized the urgency of this transition, both in its work at the Federal Communications Commission (FCC) focused on speeding this transition, and in numerous Presidential policies calling for the modernization of legacy infrastructure from the new *America First Resilience Strategy* to the *Cyber Strategy for America*. These actions echo numerous executive orders and federal policies over the past decade calling for the need to migrate away from legacy networks supporting critical federal functions. This creates greater urgency for agencies.  Private sector stakeholders are quickly transitioning to IP networks, so agencies will get the best available services if they keep up.

TDM networks, as compared to IP networks, are extremely limited in the security features they can offer and the frameworks they can adopt. In general, unlike TDM networks, IP networks support:

- **Rapid firmware patching** to upgrade software security and fix security bugs.
- **Integration with "zero-trust architectures"** that continuously verify and authenticate users and devices.
- **Encryption by default** for data, files and communications.
- **Real-time threat detection** when security attacks emerge.

Taking these realities into account, it is no longer prudent for U.S. federal agencies to wait to transition to IP networks for critical communications infrastructure.

**Modern Cybersecurity Practices Demand Networks that Support Agility and Adaptability**

While TDM-based systems have not changed much since their introduction decades ago, cybersecurity practices have. USG cybersecurity expectations for both commercial and federal networks now assume IP-based capabilities that are difficult or impossible to implement consistently on legacy TDM systems. Moving from TDM to IP is not merely a technology refresh; it is the enabling prerequisite for implementing modern cybersecurity controls at scale, which improves mission assurance, continuity of operations, and protection of public services.

Consider the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), the landmark industry-government collaboration that constitutes the most prominent consensus cybersecurity guidelines. The CSF serves as a dynamic, adaptable playbook for companies, organizations and government agencies to shape their cybersecurity practices. In trying to achieve the security outcomes outlined by CSF, IP-based services enable success while TDM-based services fall short. Ironically, by continuing to rely heavily on TDM networks, the USG is not yet able to fully implement its own consensus cybersecurity playbook.

| Core Functions | IP Networks | TDM networks | IP Networks in Practice |
|---|---|---|---|
| Identifying cyber risks | Support automated discovery, inventory, configuration management, and dependency mapping. | Lack telemetry capabilities and asset visibility, making risk management and supply-chain assurance harder. | Easier to monitor the status and health of every piece of equipment. |
| Protecting against risks | Enable modern authentication, encryption, segmentation and policy enforcement. | Limited adoption of contemporary protective controls and security structures. | Encryption of critical communications to protect against hackers. |
| Detecting attacks and compromises | Support centralized logging, network detection, and endpoint/network telemetry. | Limited monitoring and event data reduces speed and fidelity. | Track security logins in real-time and flag unusual communications. |
| Responding to incidents | Architectures integrate with incident response tooling and allow faster containment. | Often require slow, manual, specialized interventions. | When a compromise is detected, IP network traffic can be rerouted to an uncompromised segment of the network. |
| Recovery of assets and operations | Supports redundancy, diverse routing, rapid re-provisioning, and more flexible failover designs. | Lacks meaningful recovery capabilities. | Phone and data services restored within minutes after an IP network automatically fails over to a geographically redundant data center. |

Aligning with NIST's CSF only scratches the surface of the security benefits of the transition to IP-based networks. By upgrading to IP-based networks, federal agencies can patch vulnerabilities and address deeply rooted survivability and security concerns quickly.

Additionally, IP-based networks do not carry the supply chain concerns that arise when relying on decades-old parts that are no longer produced. With a competitive marketplace and multiple vendors producing necessary hardware and software, maintaining, repairing, and improving IP-based networks is significantly easier than implementing fixes to TDM networks. IP-based modernization provides benefits from assured supply chains and standardized procurement from a robust and diverse market of trusted U.S.- and ally/partner-based suppliers, allowing for alignment with NIST's Supply Chain Risk Management guidance that helps protect against risks from poor manufacturing or malicious functionality; whereas TDM resale-market sourcing undermines provenance assurance and trust.

IP-based networks also facilitate organizations' adoption of additional security and privacy controls that minimize risks associated with poor manufacturing or malicious functionality. Just as IP-based networks enable outcomes desired in NIST's CSF, they also enable the outcomes NIST's Security and Privacy Controls (SP) 800-53 were designed to provide:

- **Access control** over organization resources, data, systems, and equipment.
  - ✓ **IP:** Ensure that the only people that have access to resources are those authorized for access by authenticating user identity and authorizing access based on user permissions at different security points.
  - × **TDM:** Lacks modern enforcement at security points.
- **Audits** of user activity and system performance.
  - ✓ **IP:** Real-time access to user logs and metrics to analyze behavior and recognize anomalies.
  - × **TDM:** Lacks the data capacity to support.
- **Systems and communications protection**.
  - ✓ **IP:** Supports encryption-in-transit, segmentation, secure protocols, and modern boundary protections to keep communications and data away from compromised parts of the networks and out of the hands of bad actors.
  - × **TDM:** Constrained in adopting modern protections.
- **System and information integrity**
  - ✓ **IP:** Supports efficient patching, vulnerability management, and integrity monitoring.
  - × **TDM:** Patching, vulnerability management and integrity are more difficult, expensive and time-consuming to implement.
- **Contingency planning** to recover in the event of a cyber incident.
  - ✓ **IP:** Supports rapid restoration and tested failover.
  - × **TDM**: Restoration is slower due to parts scarcity and specialized labor.

As AI and other emerging technologies rapidly change both the cyber threat environment and defense capabilities, it is imperative that USG communications are built on technology capable of supporting and adopting the most cutting-edge innovation that keep U.S. networks a step ahead of threats. By upgrading to IP-based technology, federal agencies not only extend the lifespan of their communications infrastructure; they enhance their overall security and resilience to harden communications and operations for the future.

Beyond civilian agencies, the benefits of IP-based networks outlined above will have a meaningful impact on supporting the security and resilience of DoW missions and the defense industrial base. That benefit is clear in the context of the Cybersecurity Maturity Model Certification (CMMC) Program, which the DoW uses to assess defense contractor performance by reinforcing that cybersecurity must be demonstrable, measurable, and sustained. Where TDM increases dependence on compensating controls and legacy sustainment practices that are difficult to evidence and scale, IP-based communications better support the repeatability and evidence-based requirements that fit the CMMC – capabilities like access control enforcement, logging, and configuration and vulnerability management.

Ultimately, modern cybersecurity frameworks are intended to ensure that essential services remain trustworthy and available. IP-based modernization enables agencies to implement practices that reduce the probability and impact of outages, intrusions, and supply-chain compromise. This directly protects public-facing services (availability), sensitive data (confidentiality), and the integrity of government operations (integrity), thereby improving continuity of operations and public trust.

**Executing the IP Transition with Urgency**

Upgrading to IP-based systems is achievable; agencies that have not yet transitioned can look to successful examples of other security transitions to inform their path forward. CISA has ordered all Federal Civilian Executive Branch Agencies (FCEB) to identify and retire End-of-Support (EOS) edge devices. Step-by-step, the directive moves several agencies in the right direction, by requiring them to:

1. Immediately update edge devices running on EOS software.
2. Take stock of all devices in use that are on the CISA EOS Edge Device list.
3. Decommission those devices within one year and fully phase them out within 18 months.
4. Establish a repeatable process for identifying, decommissioning and phasing out devices in the future.

The directive from USG's leading civilian cybersecurity agency sets a clear tone, but CISA is not the only organization that is taking action. The Federal Aviation Administration (FAA) has also announced a comprehensive plan to modernize the U.S. air traffic control system and replace its current TDM-based network with an IP-based system. To execute this transition with urgency, we recommend the following steps for funding, planning, and coordination.

**Secure funding**. Funding will be a primary obstacle for the IP transition in federal networks, but given the pressing national security implications, the Administration has a strong case with Congress to make funding these upgrades a top priority. Whether through appropriations, rescissions, or reconciliation legislation, agencies with urgent requirements and fewer resources should be asking for funding now. In addition, agencies should keep in mind that:

- FCC spectrum auctions will generate billions of dollars that could be earmarked for these upgrades and fill funding gaps.

- Industry partners are also encouraging these upgrades and can serve as partners to co-invest, improving resource allocation and making further requests to Congress easier.

This approach actually will lower long-run costs. While migration requires near-term investment, maintaining TDM-based communications is increasingly expensive and inefficient over time. As legacy services age out, agencies pay a growing premium for scarce parts, specialized labor, and bespoke support arrangements — often with fewer competitive options and longer restoration times. These costs are compounded by the operational impact of outages and the security burden of compensating controls required to protect systems that cannot adopt modern security frameworks. These are sunk costs, as these networks do not have the ability to upgrade and scale as modern IP-networks can.

**Establish a dedicated office or agency to facilitate these transitions.** Without top-down senior level guidance across the government, progress on upgrades could be slow and fragmented. To inspire swift, decisive, and coordinated action, a dedicated executive branch office or agency, either within the White House or at an agency such as CISA that is empowered to push the transition, should be set up and tasked with facilitating these upgrades to ensure proper prioritization, cost-effectiveness, and timeliness. To avoid the fits and starts of previous transition efforts, appropriate authority and senior-level support must be provided to the coordination executive agency to ensure the success of the transition.

**Establish a concrete TDM sunset strategy and timeframe**. It takes time to get the job done thoroughly and correctly, but as this paper highlights, there is an urgency to execute this transition as soon as possible. The FCC has proposed this transition for U.S. commercial networks;[5] of course the U.S. government itself should lead the way. Federal agencies need to start taking inventory today of their TDM-based circuits and equipment and prioritize upgrades based on mission criticality. Agencies should also examine private sector architectures and network engineering standards and adopt next generation processes and protocols for exchanging traffic in an efficient and secure manner.  From there, agencies can find a replacement path for parts and build a replicable process to make sure that their infrastructure is always up to date.

**Require lifecycle risk assessment**. Agencies should assess whether they are relying on a strong supply chain with a healthy number of security-compliant vendors and technicians to support their systems going forward. Doing so will help avoid long-turnaround times when pieces of equipment fail.

**Remove regulatory barriers.** Infrastructure projects, especially those involving the federal government and federal lands, include extensive regulatory processes. These regulatory hurdles, such as federal permitting, slow projects down even if funding has been secured. It is important that agencies start to coordinate today to lower these barriers so upgrades can be made quickly when the time comes.

**Prepare to deploy IP-based solutions.** Facilities in remote locations are going to need tailored solutions such as microwave links or satellite technology. To ensure those options are available, coordination with industry will be key to start preparing the right solutions for each facility. This

[5] Advancing IP Interconnection; Accelerating Network Modernization; Call Authentication Trust Anchor, WC Docket Nos. 25-304, 25-208 & 17-97, Notice of Proposed Rulemaking, FCC 25-73 (rel. Oct. 29, 2025).

includes agencies directing their procurement and technology teams to engage and cooperate with vendors on upgrading existing facilities expeditiously where additional funding is not needed, but a contract change or addendum may be necessary.

**Conclusion**

Transitioning from TDM to IP-based communications is not an IT modernization preference — it is a mission assurance imperative.

Many federal missions depend on communications that are continuously available, support rapid restoration, and can be secured and monitored to current standards. As TDM services become increasingly constrained by vendor support, parts availability, and shrinking expertise, agencies face a growing risk of outages, degraded performance, and un-patchable vulnerabilities. At a certain point, keeping TDM networks running will become incompatible with meeting mission requirements — especially in this new era of enhanced cyber risk due to the sophistication of frontier AI models in detecting network vulnerabilities. Urgent migration to IP-based systems is therefore essential to sustain continuity of operations, protect sensitive communications, and ensure agencies can execute their statutory responsibilities under real-world conditions.

Decisive action to fund, plan, and execute upgrades must happen sooner rather than later. Considering the sheer size of the federal government's network infrastructure, the process is inherently slow and fragmented, but with top-down direction from senior USG leaders, agencies can overcome the challenges to upgrading agency networks to secure American infrastructure for the future.

As former senior federal officials, we have worked with USG agencies in a variety of ways for years to plan for the IP transition and to advocate for proactive planning and budget allocation to ensure adoption of IP-based communications. Most agencies have been eager for the benefits of transitioning to agile, adaptive IP-based networks, but have been handicapped by budget, contractual, or planning constraints. The time for the transition is overdue. We think it is necessary for our national security for agencies – especially those supporting national security and other essential functions – to complete the IP transition as soon as possible. With recent advances in AI technologies and network vulnerability detection, anything less may be too late to secure the survivability of those functions.