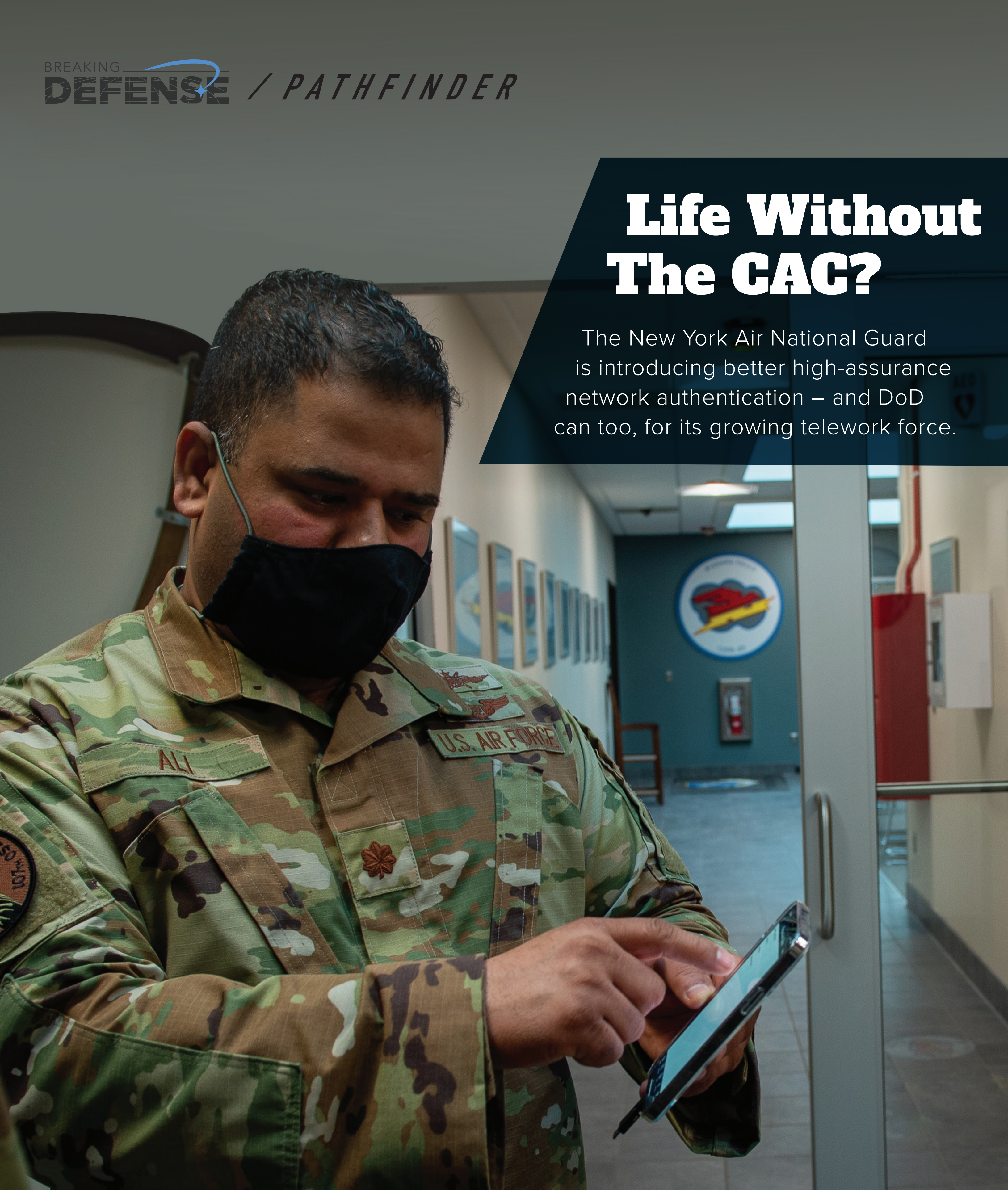
BREAKING DEFENSE / PATHFINDER

Life Without The CAC?

The New York Air National Guard is introducing better high-assurance network authentication – and DoD can too, for its growing telework force.



A BREAKING DEFENSE CUSTOM REPORT SPONSORED BY yubico

SITREP

New Tools to Secure the Expanding Network Perimeter

Defense Department IT professionals have practiced a defense-in-depth strategy for years—relying upon a series of firewalls for fundamental security against predicted and known threats. However, in today's post COVID-19 world the attack surface is changing as network access is moved out of the walled boundaries of organizations into clouds, as well as directly to individual homes of active and retired personnel.

This alters the concept of a "perimeter", making traditional security increasingly irrelevant as a way to protect networks, data, and intellectual property.

That's especially true given the proliferation of privileged accounts that give users the ability to access sensitive data and applications. The same goes for the most ubiquitous devices of all to access Department of Defense (DoD) networks—smartphones and tablets.

Together, these avenues of access have one vulnerability in common—the username-and-password login process. What's the single wall that's blocking nation states, rogue actors, and cyber criminals from hacking email accounts? It is the log-in screen with potentially weak authentication methods that result in a vulnerable cyber defense strategy.

Firewalls are no longer effectively serving that purpose. Instead, remote identity proofing, access management, and strong authentication are quickly becoming the new bulwark against cyberattacks. To see what this looks like in practice, one should examine a strong authentication solution from Yubico called the YubiKey. The YubiKey is a DoD Office of the CIO-approved hardware security key that is an alternative to the well known Personal Identity Verification (PIV) credential or the Common Access Card (CAC) that meets Federal Information Processing Standards 140-2 (FIPS 140-2). With the YubiKey, a wide range of personnel—both CAC eligible and non-CAC eligible, including reservists, coalition forces, and private contractors—can access secure DoD networks without SMS, one-time passwords, and mobile authenticators.

This approach falls in line with the stated strategy of DoD's cyber leadership to find new and better ways to secure network access.

"By making the Department of Defense Information Network (DODIN) harder to compromise, and by reducing the operational impact of compromises, our networks are becoming more resilient," said Gen. Paul Nakasone, commander of U.S. Cyberspace Command, speaking in March 2020 before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities. "This imposes a cost on adversaries because they must expend greater resources, only to reap diminishing returns. My priority for defense in 2020 is to emphasize a command-centric model so that our network defenders are threat informed and our leaders are accountable for the security of the networks they operate."

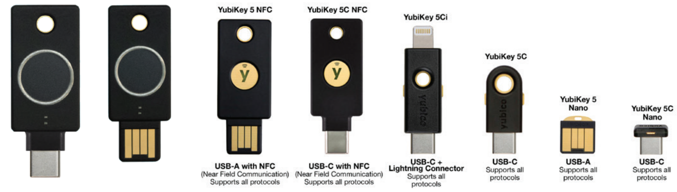
– Barry Rosenberg, Contributing Editor
Technology & Special Projects

On the cover: ***Maj. Liaquat "Rocket" Ali, Remote Piloted Aircraft Cyberspace Officer, New York Air National Guard 107th Attack Wing, demonstrates use of a YubiKey for authentication. Photo by MSgt. Brandy Fowler, NYANG, for Breaking Defense.***

The Threat Landscape

The two top data breach attack vectors today are phishing attacks and stolen credentials, according to Verizon's 2019 Data Breach Investigation Report. That means that attackers are relying less on nefarious hacking activities like worms and viruses. Instead, they simply need to steal your username and password. And when they do, studies show they often operate inside your organization, known as "dwell time", undetected for 60+ days and much longer in many cases.

To subvert the new perimeter, attackers use social engineering attacks to steal usernames and passwords. There's a long list of government agencies and private companies that have fallen prey to phishing attacks that resulted in people giving away legitimate credentials. Many of those attacks have led to privilege escalation, where attackers gained access through non-privileged accounts and maneuvered their way to higher privileges and sensitive information like defense plans, budgets, strategic planning documents, and Personally Identifiable Information/Protected Health Information (PII/PHI) that can cripple the government.



These are two new keys that Yubico is offering in preview called the YubiKey Bio. These have biometric fingerprint sensors and FIDO U2F/FIDO2 compliance.

Third-party vendors are of particular concern, as breaches from this group were the source of several significant attacks in recent years. Additionally, the cloud introduces software as-a-service and third-parties/contractors to the access landscape, along with possible unanswered questions about their security practices.

Thousands of personnel who previously never worked remotely are currently doing so from geographically dispersed environments due to COVID 19. For the DoD and other federal, state, and local government agencies, remote workers introduce new potential vulnerabilities—whether it be weak passwords on personal computers not being updated with the latest vendor security patches, poorly secured home WiFi routers, or a family member's device passing along a computer virus.

This makes military personnel with CACs potential targets for hackers. Thus authentication solutions need to be resistant to phishing and prevent account takeovers, while complying with federal regulations. The YubiKey from Yubico was specifically designed to secure against these more advanced cyberattacks that we're seeing today.

"The number one problem we're solving right now is the defense against phishing," said Yubico federal sales director Rob Konosky. "Instead of other technologies that mainly remediate after a phishing attempt, the YubiKey stops phishing based on the newer protocols that are on the YubiKey. Users don't have to determine if they're looking at a phishing attempt because the YubiKey makes that decision and will not allow the user to log in to fraudulent sites.

"Google has said publicly that they reduced account takeovers to zero after deploying YubiKeys for all their employees. That's zero percent, not 0.001 percent. So it's a significant defense against phishing."

The YubiKey is the only DoD OCIO-approved alternate hardware authenticator to a CAC that supports multiple authentication protocols and meets DoD's cybersecurity requirements. YubiKeys are approved for use in both DoD non-classified and secret classified environments.

The YubiKey is a hardware security key that only does secure cryptographic authentication. It is not a storage device like a flash drive. It comes in a variety of different form factors with some fitting on a keyring, offering NFC and lightning connectors, as well as USB-A and USB-C connectors designed to remain in the USB port.

Each YubiKey includes a secure built-in chip that accommodates derived PIV/CAC requirements, eliminating device-based authentication. A single security key can be used to securely authenticate users to applications and services across multiple government issued or personal devices such as laptops, desktops, tablets, and mobile phones. In fact, the name "YubiKey" is a play on the word "ubiquitous" because it is a single, ubiquitous device to provide security for any device that connects to the Internet. The YubiKey supports multiple authentication protocols on a single device, including the latest authentication standards such as FIDO U2F and FIDO2/WebAuthn.

"The government has mandated that users must use the CAC if they have one, but there are situations where the CAC is usable but isn't really viable because it is based on smart-card technologies from the 1970s," said Yubico solutions engineer Cody Hussey. "There are modern authentication mechanisms that are now available, specifically credentialing like Fast Identity Online (FIDO) web authentication, that really are the future.

"YubiKey does much of what a CAC does and lets the DoD take advantage of modern authentication for cloud computing and implement Zero Trust philosophies," said Hussey, noting that Yubico is a founding member of the FIDO Alliance and co-authored FIDO's Universal Second Factor (U2F) authentication. "The YubiKey is, in fact, a linchpin of the Zero Trust concept because it is the token that asserts your identity and that provides high assurance that you are who you say you are."

With the YubiKey as a portable root of trust, users can establish trust on a new device and have a portable credential to authenticate seamlessly across multiple devices; and YubiKeys don't need network connectivity, cellular connections, or batteries to work, and are manufactured securely in the U.S. using stringent processes and a secure supply chain for trustworthy components. They also ensure that air gap networks (where a secure computer network is isolated from a non-secure public network like the Internet) stay secured against breaches by providing a multi-factor authentication solution that works well in network-isolated and mobile-restricted environments. With a YubiKey, users can be authenticated without transfer of information across multiple security domains such as unclassified and classified.

Myriad Ways DoD Network Assets are Presently Secured

To better understand how YubiKeys fit into an identity proofing landscape, ensuring users can access DoD networks in a telework environment, it's helpful to look at the different ways that DoD presently requires authorized users to authenticate with DoD-approved PKI credentials. The top set of authentication methods listed just below apply to unclassified networks such as the Non-classified Internet Protocol Router Network (NIPRNet). Note that these methods address the most common form of access for the majority of active duty users—the Common Access Card— as well as different credentials for privileged users, who are those with higher access clearance, working with more sensitive data and applications, as well as those used by close coalition partners and allies.

The bottom set of authentication methods apply to secret classified networks such as the Secure Internet Protocol Router Network (SIPRNet). Note the accommodations for users at other federal agencies and the Five Eyes partners (Australia, Canada, New Zealand, the UK).

NIPRNet

1. Common Access Card (CAC): This is the primary DoD PKI credential for logical authentication to unclassified DoD networks, systems, servers, and applications. The CAC meets the criteria for Authenticator Assurance Level (AAL) 3 in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, Digital Identity Guidelines.

2. NIPRNet Alternate Logon Token (ALT): The DoD ALT is the mandated DoD PKI credential for authentication to privileged user accounts on the NIPRNet. The ALT is also used for group and role accounts, and may be used for NIPRNet logon in accordance with DoD policy. Amazon Web Services defines a "group" as primarily a convenience to manage the same set of permissions for a set of users. A "role" is an entity with permissions to make service requests.

3. External Certificate Authority (ECA) PKI Credentials: ECA medium token assurance and medium hardware assurance PKI credentials are used to authenticate to unclassified DoD information systems, and are not used for network logon and authentication to privileged-user accounts. They meet the requirements for AAL3.

4. Personal Identity Verification (PIV) PKI Credentials: These also qualify as AAL3, and are used for both network logon and authentication to unclassified DoD information systems on unclassified DoD networks.

5. PIV-Interoperable (PIV-I) and Industry Partner PKI Credentials: These credentials are used to authenticate to unclassified DoD information systems but not for network logon and authentication to privileged-user accounts. They qualify as AAL3.

6. Five-Eyes (FVEY) Mission Partner PKI Credentials: FVEY users must use either ECA Medium Token Assurance (or above) PKI credentials or their own unclassified PKI credentials to authenticate to unclassified DoD systems. Unclassified FVEY PKI credentials must be issued under a FVEY unclassified PKI Root Certificate Authority (CA) cross certified with a DoD PKI.

SIPRNet

1. National Security Systems (NSS) SIPRNet PKI Token: This is the primary credential for logical authentication to Secret classified DoD networks, systems, and applications.

2. DoD NSS SIPRNet PKI Admin-I Token: This is the mandated DoD PKI credential for authentication to DoD administrative accounts on SIPRNet.

3. Federal Partners: NSS PKI tokens from other federal departments and agencies are approved for authentication to SIPRNet DoD resources provided that the federal entity has connected their NSS secret classified network to the SIPRNet via the Federal Demilitarized Zone (FED DMZ) in accordance with the DoD CIO memorandum, "Improving Security of Federal Department and Agency Connections to the DoD SIPRNet FED DMZ."

4. Contractors at Contractor Facilities: DoD contractors who access the SIPRNet via contractor-facility enclaves must obtain NSS SIPRNet PKI tokens from their DoD Component sponsors.

Telework Demands Alternate Authentication

Oftentimes, personnel without the above-named credentials and authentication capabilities have legitimate needs to access DoD networks. For example, short-term contract workers that aren't eligible for a PIV credential or CAC may also require secure access to government services and systems.

This category also includes retired military personnel, reservists, and members of the Army and Air Force National Guards. These people often have civilian jobs while serving part time on the weekend.

Very few Reserve and Guard personnel are issued government-furnished equipment (GFE), unless they are key/essential personnel or have special authorization, to permit access to less-sensitive NIPRnet applications. Although all Reserve and Guard members are issued CACs, their CAC credentials are of little use without a government issued laptop/PC or a CAC reader to access DOD sites. In addition, retirees only get plastic cards with barcodes that are used to enter military installations, shop at a commissary or base exchange, and can be used as a source of identification for other military benefits such as healthcare, billeting, and recreation services.

That is the case at the New York Air National Guard and all the others nationwide. As a state militia, the New York Air National Guard operates outside the U.S. Air Force chain of command. National Guards operate under the jurisdiction of individual state governors unless they are federalized by the president.

To meet the needs of National Guard personnel and others, the Defense Department has approved the use of three other multi-factor authentication (MFA) solutions when PKI is infeasible. And that's where Yubico's YubiKey fits in. It makes it possible for personal non-GFE devices in a bring-your-own approved-device (BYOAD) environment to be authenticated to DoD networks. "DoD-approved multi-factor authentication may only be

As in other domains of warfare, forces in Reserve and Guard components can augment active duty forces for Title 10 missions that include cybersecurity. Shown is an Air Force airman assigned to the 609th Air Operations Center inside the Combined Air Operations Center at Al Udeid Air Base, Qatar.

The National Guard and Reserve can be force multipliers in the DoD's cybersecurity efforts. Shown is a C-130J from the California Air National Guard delivering 200 ventilators to the 105th Airlift Wing of the New York Air National Guard at Stewart Air National Guard Base, Newburgh, NY, in April 2020.

used when either a system or application does not support authentication using DoD-approved PKI credentials, or a portion of the system or application's subscribers are unable to obtain DoD approved PKI credentials," states the 2018 DoD memorandum "Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems."

Federal agencies are similarly directing agencies to look for alternate authentication methods, especially when they aren't able to issue credentials during the time of remote work. In March 2020, a White House Office of Management and Budget directive told agencies to use the breadth of available technology capabilities to fulfill service gaps and deliver mission outcomes, and also to be prepared to issue an alternate credential or authenticator for physical and logical access.

Pilot Program on Authentication at New York Air National Guard

As mentioned earlier, the YubiKey is one of the three DoD-approved alternate MFA authenticators that meet DoD's rigorous cybersecurity requirements and can be safely mailed directly to users, offering YubiKey holders secure access to both unclassified and secret classified DoD information systems. (The second alternate solution also offers NIPRnet and SIPRnet access while the third is for NIPRNet only).

One of the first programs to introduce YubiKey to the military begins early 2021 at the New York Air National Guard, which operates out of six air bases and facilities throughout New York State. It conducts: airlift missions with the C-17 Globemaster III, HC-130J Combat King II, and LC-130H Hercules; attack missions with the the MQ-9 Reaper remotely piloted aircraft; rescue missions with the HH-60G Pavehawk and HC-130N Combat King; and warning and control missions for NORAD (North American Aerospace Defense Command).

It's the involvement of the National Guard and Reserve in cybersecurity that can be a force multiplier to the DoD's greater efforts in this area.

"Over the coming year we will engage the services to continue building a manpower model to support retaining the most talented (cybersecurity) professionals," said Nakasone to the House committee. One of the most impactful components of that manpower model is the reserve component."

As in other domains of warfare, forces in Reserve and Guard components can augment active duty active-component forces for Title 10 missions. Members of the Air National Guard already augment a full-time National Mission Team and two Cyber Protection Teams. The Army National Guard mobilizes more than 150 cyber personnel to defend Army infrastructure as Task Force Echo. And for additional cyber capacity, the Army is building 21 Cyber Protection Teams across the Reserve and Guard.

Said Nakasone: “The Air Force Reserve and Navy Reserve provide additional augmentation to active duty Cyber Protection Teams and Combat Support Teams. Their value to the nation is increased by the leadership and experience of so many of these individuals in the private sector. Since over 80 percent of critical infrastructure is in the private sector, members of the Guard and Reserve are a valuable source to bridge the knowledge between the government and private sector. There is much experience to be shared between the C-suite and the command suite.”

As part of those efforts, the New York Air National Guard in conjunction with the New York State Division of Military and Naval Affairs are scheduled to begin a test program in 2021 that employs YubiKeys to let guard members authenticate to a New York State emergency management system, and progressively to DoD CAC credential-enabled sites with personnel, financial, and healthcare services.

“The DoD’s secure system with the CAC works well but moving forward we need better authentication, especially for people who are no longer actively serving in the military and lose the ability to use a CAC,” said Maj. Liaquat “Rocket” Ali, Remote Piloted Aircraft Cyberspace Officer at the New York Air National Guard, who is one of the leaders for the YubiKey test. “For example, we use the military myPay website for financial services that require a CAC if you are still actively serving in the military. However, once you retire and lose your CAC, retirees must access myPay using username and password. MyPay recently added text and email codes as additional multi-factors features but the service can be problematic in mobile and internet constrained settings.

“We forget the retirees,” Ali told Breaking Defense. “I think sometimes we only focus on the 650,000 people we have currently in the total force, and forget about the millions of people that are already retired and their family members that need access to secure medical information, paychecks, and digital transactions. With the YubiKey, they would be able to better secure their accounts with strong multi-factor authentication.”

For active service personnel, the YubiKey can serve as an alternate authenticator to their CAC by supporting derived credentials, i.e. DISA Purebred. This is especially important for use cases such as BYOD/BYOAD, mobile authentication, and authentication for isolated/closed networks. Additionally, YubiKeys are highly suitable for a telework environment, where users may not have CAC readers on their non-GFE devices.

The New York Air National Guard test will start small by giving YubiKeys to about 15 senior leaders so they can have immediate, secure access. The plan is to then add 50 more users and then 1,700 users by the end of first quarter 2021. Success will be measured by users’ ability to securely login using the YubiKey as an additional factor of authentication and as an alternative to a physical CAC card.

“Air Force Vice Chief of Staff Gen. Stephen Wilson has said that 30 percent of the force might continue to work remotely going forward,” said Ali. “We need to figure out ways for them to work securely without having to physically go to a base. In other words we need a virtual base.

“This protects the security of the military but also gives you the flexibility to meet the demanding needs of COVID 19 or whatever might come next. I want to be able to fight my battle with smart people from all over the world by getting them network access to help me execute our missions. That is the future vision.”

The Takeaway

Remote work is here to stay for the foreseeable future, and will inevitably change how some employees work in the long-term. The current pandemic situation has forced this digital transformation at an accelerated rate, driving remote work scenarios for tens of thousands of DoD personnel.

Recognizing that reality, the DoD and federal government agencies are working to fast track secure easy-to-use authentication to ensure that remote workers connecting to government networks and cloud-hosted services do not leave open doorways for cyber criminals to exploit.

By mitigating cyber security threats such as phishing and account takeovers with highest-assurance authentication, hardware security keys such as the YubiKey will help the DoD ensure the security and confidentiality of its networks and data.

A hardware key that has USB-A, USB-C, NFC and lightning form factors that don’t require a specialized reader, and the ability to be mailed directly to residential addresses across more than 30 countries, YubiKeys are a high-assurance, DoD-authorized hardware authentication security solution that can be rapidly and easily deployed to remote government workers.