AIR WAR COLLEGE

AIR UNIVERSITY

OPTIONS FOR ADDRESSING AIR FORCE CYBER NEEDS IN THE FACE OF LIMITED RESOURCES

by

Martin Jennings, Lt Col, USAF

Muir S. Fairchild Research Information Center
Digital Collections
University–Maxwell AFB

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Clint Mixon, Col, USAF

14 March 2018

DISTRIBUTION A. Approved for public release: distribution unlimited.

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Biography

Lt Col Martin Jennings is assigned to the Air War College, Air University, Maxwell AFB, AL. He received his commission upon graduating from Officer Training School in 1998. Prior to his commissioning, Lt Col Jennings was an enlisted programming specialist. He is a Master Cyber Operations Officer with over 26 years of cyber, communications and information experience. Lieutenant Colonel Jennings has served in staff assignments on the Joint Staff, as an Action Officer working Cyber Mission Force training and manning issues and at HQ Air Force as an Action Officer working Enterprise Email and Information Management solutions. He was the Chief of the Director's Group at the Defense Information Systems Agency where he worked strategic programs and special projects including the Joint Information Environment. Lieutenant Colonel Jennings has extensive operational experience including deployments in support of Operation IRAQI FREEDOM as part of the Multi-National Force-Iraq staff, on the USS Blue Ridge as part of Joint Task Force-519, and to Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates in support of Operations SOUTHERN WATCH and DESERT FOX. Lt Col Jennings has also commanded two units at the Squadron level.

Digital Collections

Abstract

The Air Force is facing growing cyber resource requirements and must find innovative ways to free up manpower and money in the face of sequestration. This paper provides two options for freeing up cyber resources while maintaining or improving the Air Force's cybersecurity posture. The first option is to engineer a solution for network security based on Google's BeyondCorp solution. The core tenet of this solution is the elimination of trusted network segments and reliance on device and user identity management to provide a tiered trust solution for accessing secured resources. The second option advocates for increased speed of adoption of cloud solutions and Joint Information Environment enterprise solutions such as Defense Enterprise Email.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Introduction

The Air Force, along with the other Services, organize, train and equip and present cyber forces to United States Cyber Command to conduct military operations in support of Combatant Commands and joint force commanders worldwide. According to the Joint Staff-led Cyber Force Management Tiger Team, "Over the past four years, the Air Force has struggled to present their portion of the Cyber Mission Force due to manpower shortages, attrition, and competing service priorities."[1] The Defense Management Advisory Group recently approved the manpower and organizational structure for the command and control force that supports and directs the Cyber Mission Force.[2] This 2019-2023 manpower requirement is above and beyond the current Cyber Mission Force and Air Force internal cyber requirements.

The Air Force has a history of finding unique manpower solutions in the form of career field mergers and by revectoring career fields away from missions that could either be outsourced or eliminated. As Maj Gen Weggeman (Commander, 24th Air Force) recently testified to the Senate Armed Services Committee's Subcommittee on Cybersecurity, "manpower deficiencies in our units that operate, secure, and defend our networks still force a constant high-pressure deployed-in-place operating environment of competing priorities and risk decisions with insufficient force structure to meet critical operational demands. The Enterprise Information Technology as a Service effort will help alleviate some of this burden."[3] While he cautioned that Enterprise Information Technology as a Service would not be a panacea, he stated that eliminating the requirement for Air Force cyber operators to perform traditional information technology and network operations (fixed force defense) missions would free up much needed cyber manpower to support other critical missions. This paper will provide several options for

how the Air Force could leverage automation and the cloud to free up additional cyber resources to meet the needs of United States Cyber Command and its internal cyber missions.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Thesis

Given the 2017 Defense Management Advisory Group approved Cyber Mission Force command and control model, what are some of the options for the Air Force to optimize the use of its limited cyber resources in support of organize, train and equip efforts for the Cyber Mission Force, Cyber Mission Force command and control and traditional cyber requirements? This research paper argues the benefits of accelerating to the cloud and eliminating our reliance on an antiquated Maginot Line-like approach to cyber defense. Acceleration to the cloud and eliminating our traditional approach to Non-classified Internet Protocol Router Network (NIPRNET) management and defense will free up needed cyber resources.[4] The freed manpower and dollars can then be used to both resource the Cyber Mission Force and Cyber Mission Force command and control requirement levied by the Department of Defense and flesh out the Air Force Chief Information Officer Cyber Squadron Initiative focused on mission assurance of the Air Force's core missions. This change in approach will free up these needed resources and make our cyber defense posture more secure because it will eliminate the need to operate and maintain base level communications, long-haul circuits and enterprise services such as email; will eliminate our reliance on a Maginot Line-based defensive posture; and will focus on defending core mission systems and end-user authentication.

Digital Collections

The Cyber Demand Signal

The recent Presidential decision to elevate United States Cyber Command to Combatant Command status underpins the importance that the burgeoning cyber domain is having on Joint warfare. As part of their inherent organize, train and equip functions, the Services currently provide 7,963 personnel in support of United States Cyber Command's mission[5] to conduct military operations in support of all Combatant Commands and joint force commanders worldwide.

The structure and target composition of the primary 133 Cyber Mission Force teams have been the primary focus since their inception in 2013.[6] Accordingly, the Services have focused their efforts in support of United States Cyber Command on identifying, training and equipping the necessary forces. Their goal is to fully field the required 6,187 personnel by Sep 30, 2018 to meet the full operating capability criteria[7]. Thus far, all the Services have met their Initial Operating Capability goal (Sep 30, 2016) and have been able to present roughly 4,900 of the 6,200 personnel required.[8] As of December 2017, the Army and Navy have reached full operating capability, and the Marines are one team away from attaining full operating capability. Based on Joint Staff projections, without a significant change in how the Air Force currently organizes, trains, equips and employs cyber manpower, the Air Force could miss the full operating capability deadline of Sep 2018.[9]

To further compound the Air Force's cyber organize, train and equip issues, the process of elevating United States Cyber Command and fleshing out the command and control headquarters structure will require another 1,295 cyber and intelligence personnel from 2019-2023.[10] The Joint Staff and the Department's Principal Cyber Advisor led an effort in 2016 to define the manpower required for these organizations. Manpower Assessment Teams completed

studies at United States Cyber Command and all its subordinate headquarters (Joint Force Headquarters-Cyber National Mission Force, Joint Force Headquarters-Department of Defense Information Networks, the four Joint Force Headquarter-Cybers, and the nine Combatant Command Integrated Planning Elements) that Command and Control the Cyber Mission Force.[11] The June 2017 Defense Management Advisory Group decision codified the results of these manpower studies and provided manpower guidelines for the Services to resource from 2019 to 2023. This Defense Management Advisory Group decision levied another Department of Defense cyber manpower burden on the Air Force[12] that will need to be reconciled with service cyber manpower constraints. The Secretary of the Air Force Chief Information Officer, Cyber Squadron Initiative and the need to provide enterprise network services to Air Force users represent additional manpower challenges that the Air Force is in the process of reconciling.[13]

This manpower burden comes while the Air Force already faces a shortage of cyber manpower with few options to increase capacity. According to the Air Force Personnel Center, the officer and enlisted cyber career fields are unable to sustain current validated requirements much less the additional requirements levied by the 2017 Defense Management Advisory Group.[14] AF/A1 recommends reviewing and revalidating all cyber requirements to identify positions that no longer require cyber personnel and to rebalance the cyber force with appropriate grade distributions.[15] This rebalancing is required because the projected demand for cyber manpower in traditional information technology jobs across the Air Force has not drawn down at the rate expected from PBD 720 actions.[16]

To help accelerate the reduction of traditional cyber requirements, the Air Force is pursuing "as a service" initiatives at both the base and enterprise levels leveraging industry to provide communications and information technology services. Today, Communication

Squadrons, Network Operations and Security Centers and specialized squadrons enabling specific Air Force missions, provide this service. "As a service" initiatives seek to transfer these responsibilities to industry via contracted service providers. In theory, this "initiative" provides more effective communications and information technology services, while simultaneously refocusing Airmen to assure the Air Force's core missions in contested cyber environments.[17]

To assist with assuring these missions, SECAF and CSAF Strategic Guidance, dated 4 Feb 2016, directed the creation of Cyber squadrons to focus on mission assurance to provide active cyber defense capabilities in support of wing commander missions. This guidance was echoed in a 29 June 2016 AF/CV memorandum titled "Operating In, Thru, and From Cyberspace" in this memo, the AF/CV concluded that embedded cyber forces will be necessary to generate and project combat power, employ air forces, and create effects in all domains. In response to this direction, the Secretary of the Air Force Chief Information Officer/A6 announced the Air Force Chief Information Officer Cyber Squadron-Initiative.[18]

According to this initiative, future Cyber Squadrons will require a fundamental restructuring of the Air Force's cyber community so that it is tailored to the needs of the wing commander's mission while preserving the Air Force's ability to provide communications and information technology services. Further, as the need for fixed force defenders such as Mission Defense Teams grows, much of the information technology force will be cross-utilized to perform these functions out of hide. According to the Deputy Commander of Air Force Space Command, the fixed force defenders are different than the maneuver force employed by the Cyber Mission Force in that they are cyber defense personnel that are focused on the defense of the internal Air Force portion of the Department of Defense Information Networks, Air Force weapon systems and the operational technology used to operate bases.[19] A new method of

securing Air Force networks could help drive efficiencies by bringing the duties of the fixed and maneuver forces closer together.

Efforts by United States Cyber Command to establish the Cyber Mission Force and associated Cyber Protection Teams were intended to address the proliferation of cyber threats, but their evolution has highlighted the need for an organic Air Force cyber force focused on defending the mission relevant cyber terrain of operational wings. Cyber Protection Teams can augment enclave defense but do so primarily as a maneuvering capability that is limited in scope and time. This contrasts with a Cyber Squadron that will provide persistent cyberspace security and defense capabilities to address high-end Advanced Persistent Threat actors. Furthermore, in a contested environment, the Cyber Protection Teams' mobility will be in jeopardy. Embedding cyber defenders with operational missions at isolated/contested locations is the only way to assure combat power.[20]

Digital Collections
Air University–Maxwell AFB, AL

Google's Approach

The Air Force like all military and most corporations uses firewalls to enforce perimeter security and protect their cyber assets. However, this security model is problematic because, when that perimeter is breached, an external attacker becomes a trusted insider with easy access to network assets. This flawed approach relies on security perimeters to keep attackers out but does little to track and validate activity on the inside of the trusted network.[21] As the Air Force adopts more mobile and cloud technologies, this security model becomes increasingly difficult and costly to secure. One method to both secure Air Force information and free up cyber resources entails looking at novel solutions that leverage machine learning and solid identity management principles to automate the NIPRNET security burden.

Google has developed a novel approach that is worth additional study. They eliminated their reliance on a privileged intranet, eliminated firewalls, and moved all their applications into the publicly accessible cloud. "Since the early days of IT infrastructure, enterprises have used perimeter security to protect and gate access to internal resources. The perimeter security model is often compared to a medieval castle: a fortress with thick walls, surrounded by a moat, with a heavily guarded single point of entry and exit."[22] Much like the Air Force's current approach, anyone attempting access from outside the wall was considered dangerous, while anyone located inside the wall was trusted. According to Google research, this perimeter security model works well when all of a company's employees work in a handful of buildings owned and operated by the corporation. However, with the introduction of mobile applications, the explosion of devices used by this workforce, and the demand for cloud-based services, the traditional firewall model has been stretched to its breaking point. The myriad of entry points and attack vectors further challenge this traditional paradigm and make it unwieldy to manage and properly secure.

"Key assumptions of this model no longer hold: The perimeter is no longer just the physical location of the enterprise, and what lies inside the perimeter is no longer a blessed and safe place to host personal computing devices and enterprise applications. While most enterprises assume that the internal network is a safe environment in which to expose corporate applications, Google's experience has proven that this faith is misplaced."[23] According to Google research, we should assume that an internal network is as fraught with danger as the public Internet and we should be securing our enterprise applications appropriately.

Google's BeyondCorp initiative was a seven-year endeavor that allowed them to move to a new model that dispensed with the need for a privileged corporate intranet.[24] According to Google research's white papers, they developed an identity management solution that authenticates the device as well as the user's identity and authorizes the user's access to a given application or piece of data based on role and normal activity patterns. Google's employees use the same authentication methods and pathways whether they are access resources from a Google office, a home network, or even a coffee shop. "All access to enterprise resources is fully authenticated, fully authorized, and fully encrypted based upon device state and user credentials."[25]

Google can enforce fine-grained access to different parts of enterprise resources. As a result, all of their employees can work successfully from any network, and without the need for traditional VPN connections into privileged networks. The user experience between local and remote access to enterprise resources is effectively identical, apart from potential differences in distant end latency.[26]

Google's solution is based on the concept of a "managed device," which is a device (a PC, mobile phone, tablet, etc.) that is procured and actively managed by Google. Only these

managed devices are authorized access to trusted applications. Google leverages a device tracking and procurement process that centers around a device inventory database. This database is much more than the asset tracking databases that the Air Force currently uses. At Google, as a device progresses through its life cycle, from procurement to production, Google tracks all changes made to the device. This information is monitored, analyzed, and made available to other parts of Google solution. This inventory provides Google with a single source of data about all devices that are authorized access to the Google enterprise.[27]

All managed devices need to be uniquely identified in a way that references the record in the device inventory. Google uses device certificates stored in the Trusted Platform Module (TPM) or equivalent certificate store on the device. Once the certificate is installed, it is used in all communications to Google services. While the certificate uniquely identifies the device, it is not the sole source of authentication on the device. This certificate actually provides access to a secure set of information about the device that forms the foundation of authentication at the device level.[28]

Device authentication is only one component of the solution. Google also tracks and manages all users in a central identity database. This database is tightly coupled to Google's Human Resource database. This integration provided detailed information about a given user's job role, usernames, and group memberships. Google employee data is constantly updated from the day they join the company, through job changes and promotions until they leave the company. This employee data forms the basis for the authorization engine that validates a need to access certain systems and data across Google's enterprise.[29]

Google's in-house enterprise consists of an unprivileged network that very closely resembles an external network. All client devices connect to this network when physically

Digital Collections
Air University–Maxwell AFB, AL

located inside a Google building. "For both wired and wireless access, Google uses RADIUS servers to assign devices to an appropriate network, based on 802.1x authentication."[30] Google uses dynamic, rather than static, VLAN assignments. This approach offloads the configuration burden of maintaining switch/port static configurations to an automated solution that informs the switch of the appropriate VLAN assignment for a given device. Managed devices provide their authentication certificate as part of this 802.1x handshake and are assigned to the appropriate VLANs. Any unrecognized and unmanaged devices are automatically assigned to a guest network.[31]

All Google applications and databases are exposed to both external and internal users via an Internet-connect access proxy. This proxy enforces encryption between the client and the target application or server. "The access proxy is configured for each application and provides common features such as global reachability, load balancing, access control checks, application health checks, and denial-of-service protection."[32]

The level of access given to a user and a device changes given the specific set of credentials provided and the circumstances of the request. "An Access Control Engine within the access proxy provides service-level authorization to enterprise applications on a per-request basis."[33] By fusing information from multiple sources including the requested target information, Google's access gateway can compute the level of trust authorized to the user/device pair in real-time. This level of trust is also impacted by the current state of the device. For example, a device that has not been fully updated with a recent OS patch might only be given a reduced level of trust. A specific model of phone or tablet or a user accessing applications from a new device or location might be assigned a different trust level. Google uses both static rules and heuristics to ascertain these levels of trust.[34]

Trust levels are organized into tiers and assigned to each device in real-time. Each target resource is associated with a minimum trust tier required for access by a Trust Inferer. "In order to access a given resource, a device's trust tier assignment must be equal to or greater than the resource's minimum trust tier requirement." As a device is allowed to access more sensitive data, Google requires more frequent tests of user presence on the device, so the more they trust a given device, the shorter-lived its credentials become. Therefore, limiting a device's trust tier to the minimum access requirement it needs means that its user is minimally interrupted. In addition to providing tier assignments, the Trust Inferer also supports network segmentation efforts by annotating which VLANs a device may access.[35]

While many of the components of the Google solution are familiar to military networks, a great deal of engineering and integration would be required to fully realize an equivalent capability. Google now offers their solution as a service called the Cloud Identity-Aware Proxy (Cloud-IAP). However, Cloud-IAP can currently only control access to applications hosted on the Google Cloud Platform.[36] I am not advocating for wholesale procurement of the Google service as a sole source solution. Rather, I believe the components detailed above can be used to guide Joint Information Environment solutions as well as shape engineering efforts underway for the AF Enterprise Information Technology as a Service initiative. Regardless of the specific solution, effort and dollars need to be invested in automating how the Air Force secures its networks, applications, and data.

Digital Collections

Recommendations

Given the competing priorities above, the Air Force must find innovative methods to offload traditional network management requirements while providing a more secure cyber environment. This environment must allow for freedom of maneuver of United States Cyber Command directed Cyber Mission Forces to defend critical infrastructure, generate cyber effects in support Combatant Commander missions and protect assets supporting Air Force missions.

My research provides several options for accelerating the transition to cloud-based services and eliminating the Air Force's reliance on segmented network defenses. Acceleration to the cloud and eliminating our traditional approach to network management and defense will free up critical resources. This freed manpower and dollars can be used to resource the Cyber Mission Force and Cyber Mission Force command and control requirement levied by the Department of Defense while fleshing out the Air Force Chief Information Officer Cyber Squadron Initiative in support of the Air Force's core missions.

This change in approach will not only free up needed resources; it will also eliminate the need to operate and maintain base level communications provisioning, long-haul circuits and enterprise services such as email. Additionally, leveraging best practices from industry leaders such as Google will allow us to shift our security model away from a reliance on firewalls and segmented networks toward a security model rooted in device and user non-repudiation.

First, I recommend that the Air Force eliminate its reliance on a segmented network defensive posture. The Air Force should look at best practices from industry leaders such as Google. They do not rely on firewalls and treat all network segments as untrusted. They utilize a myriad of custom solutions to protect data at rest and in motion, validate end-user devices, authenticate users, grant access to resources and control application access. They also use big

data analytics tied to machine learning to analyze user activity and validate the need for a given user, from a given device to access data or take a requested action. By architecting their cyber ecosystem with security and non-repudiation at the core, they both assure their data and reduce the manpower required to defend their resources. As the Air Force embarks on an effort to contract out base level information technology service delivery, I recommend working with NSA and United States Cyber Command experts to design requirements for this new security architecture based on industry best practices. These architectural requirements should be the basis for Air Force networks of the future and be aligned with the Department of Defense Chief Information Officer's Joint Information Environment initiative.

Second, I recommend that the Air Force join the Department of Defense effort to transition to the cloud. Focus on Infrastructure as a Service and Platform as a Service opportunities initially as these allow for the Air Force to maintain access to lower level platform and infrastructure layers required for current defensive methods. Air Force procured cloud solutions need to specifically enable Cyber Defenders to detect, deny, and defeat malicious cyber activity in each cloud computing environment. Acceleration to the cloud will increase flexibility, reduce manpower costs, and reduce investment in Air Force owned and operated equipment. Driving Air Force systems and data to the cloud will also eliminate stovepipes and data silos allowing for greater data analytics and analysis. These efficiencies also promise to drive manpower savings through elimination of manual tasks and human-in-the-loop integration that is required by of many of our legacy processes and systems.

These shifts will bring the defensive focus of both our fixed force defenders (Cyber Squadrons and Mission Defense Teams) and our maneuver force defenders (Cyber Mission Force Cyber Protection Teams) into closer alignment allowing for cross-utilization of tools,

Digital Collections

training, and planning capabilities. The shift will also eliminate the Department of Defense's reliance on a flawed cyber-security model that assumes that users and devices on the inside of the firewall are trusted and will focus on defending core mission systems through trusted hardware and end-user identity management methodologies.

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Challenges

As the Air Force and DoD accelerate to the cloud, there will be significant challenges in the form of resource constraints, Information Assurance policies and acquisitions delays. The Air Force does not have the luxury of continuing to use strained cyber resources to engineer, develop, operate, or support its own home-grown solutions for Enterprise solutions, cloud hosting or boundary protection. Objective 2.1 of the Air Force's Information Dominance Flight Plan specifically identifies this challenge and mandates the following actions.

> "Evaluate, resource, and employ cloud services that enable mission assurance... Avoid development of unique Air Force application solutions; employ industry/commercial solutions. Evaluate, resource, and employ software, platform, and infrastructure 'as a service' solutions that focus on mission assurance and cybersecurity of Air Force core missions. Consolidate duplicative and interrelated systems into a single enterprise level capability. The Air Force will migrate from legacy technology where operationally relevant."[37]

Accordingly, the Air Force should make every effort to rapidly adopt Department of Defense enterprise services and cloud-based offerings deployed as part of the Joint Information Environment. The value of leveraging cloud solutions hosted by the Defense Information Systems Agency such as Defense Enterprise Email, the Defense Enterprise Portal Service, and other Joint Information Environment applications is that they are already proven and have been engineered to work worldwide.[38] Further, many of these solutions are cheaper than an Air Force-only solution given the scale and volume discounts negotiated by the Defense Information Systems Agency.

Utilization of these Department of Defense cloud-based offerings also limits the impact of Information Assurance paperwork associated with the Risk Management Framework. As the Department of Defense's enforcer and inspector of Risk Management Framework compliance[39], the Defense Information Systems Agency can leverage its expertise to provide and assure the

Digital Collections

most secure solutions without Air Force manpower or contracted Information Assurance investments. By utilizing these hosted enterprise services, the Air Force will have access to secure cloud-hosted solutions with included Information Assurance support.

Leveraging existing Department of Defense solutions also offers a great deal of benefit when dealing with the acquisitions challenges associated with current Department of Defense policy. Buying into existing Defense Working Capital Fund solutions allows the flexibility to purchase solutions rapidly as the acquisitions work has already been accomplished by the Defense Information Systems Agency's information technology contracting organization. The primary complaint that Services have with leveraging Defense Working Capital Fund solutions is the annual price fluctuations.[40] To address this challenge, I recommend working with the Department of Defense Chief Information Officer to develop policy related to Joint Information Environment enterprise services. The policy should mandate the use of Joint Information Environment enterprise services and impose timelines for adoption.

As part of this adoption framework, the Services would be forced to utilize the same services used by the Combatant Commands they support. During a specified adoption window, all users would leverage the Defense Working Capital Fund. However, the new policy would mandate a transition to programmed operations and maintenance funding lines at the five-year point. The Department of Defense CAPE office would then transfer service funding offsets to the Defense Information Systems Agency's budget and program mandatory annual reductions in the funding line to force innovation and efficiencies. This policy would align all of the Services on a common set of enterprise cloud services while addressing the Services' concerns over Defense Information Systems Agency costs.

Conclusion

The Air Force's cyber resources are stretched thin trying to support base-level missions and United States Cyber Command Cyber Mission Force requirements. The addition of 2019 to 2023 manpower requirements supporting the Cyber Mission Force command and control structure will increase the strain on the cyber force. Additionally, there is no corporate relief from AFPC or HAF/A1 because of the current pilot shortage and sequestration impacts.[41] Given these facts, the Air Force Chief Information Officer has opted to look for efficiencies through innovative information technology solutions.[42]

This paper provided several options for how the Air Force could free cyber resources for use in support of critical wing missions, United States Cyber Command and Air Force Chief Information Officer initiatives such as Cyber Squadrons and Mission Defense Teams. These options include accelerating the transition to cloud-based services provided as part of the Joint Information Environment and eliminating the Air Force's reliance on segmented network defenses.

Leveraging corporate solutions such as Google' BeyondCorp approach to eliminate segmented network defenses as engineering blueprints for future Air Force networks will allow us to offload manpower intensive, base level management and configuration efforts. Engineering a holistic solution patterned after the Google approach would not only free resources but make the network more secure through automated VLAN assignment, tiered access, and role-based access to network resources.[43]

Additionally, speeding the adoption of Joint Information Environment enterprise services such as Defense Enterprise Email will allow the Air Force to save money and reduce manpower requirements required to operate and support the current Air Force Area Processing Center

Air University Digital Research Information Services Center
Air University–Maxwell AFB, AL

hosted solutions. These services also provide cost savings in Information Assurance and program management and Global Address List integration and have been centrally procured in order to avoid a lengthy acquisition timeline. In fact, because the Defense Information Systems agency leverages its Defense Working Capital Fund authority, funding the services is rapid and requires little more than a transfer of funds. Regardless of the final solution the Air Force must adapt to the changing cyber landscape and free up strained cyber resources. The Air Force must do this so that it can continue to support the "conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[44]

Muir S. Fairchild Research Information Center
Digital Collections
Air University–Maxwell AFB, AL

Notes

[1] Joint Staff J6 CFMITT Slides, Air Force build status slide.
[2] DMAG June 7, 2017 decision.
[3] Maj Gen Weggeman March 13, 2018 testimony p 19.
[4] Ibid, p 6.
[5] Derived from the HQ USCYBERCOM Manpower Requirements Assessment Report (1 Nov 2016) and the June 7, 2017 DMAG decision briefing.
[6] Joint Staff J6 CFMITT Slides, back up slides showing historical build data.
[7] Joint Staff J6 CFMITT Slides, back up slides detailing USCYBERCOM CMF Build FOC criteria.
[8] Joint Staff J6 CFMITT Slides, CMF Build IOC status slide.
[9] Joint Staff J6 CFMITT Slides, Services build projection slide.
[10] DMAG June 7, 2017 decision.
[11] Joint Staff J1-led USCYBERCOM and JFHQ Manpower Assessment Reports.
[12] DMAG June 7, 2017 decision.
[13] Maj Gen Weggeman March 13, 2018 testimony p 5.
[14] Derived from AFPC Health of the Cyber Career field brief, Cyber DT outbrief slides, and interview with Lt Col Dave Nuckles (HAF/A1)
[15] Interview with Lt Col Dave Nuckles (HAF/A1)
[16] Interview with Ms. Teresa Salazar (Joint Staff/J6)
[17] Ibid, p 6.
[18] SAF CIO-A6 Info Dominance Flight Plan, p 24.
[19] Maj Gen Skinner, America's Air Force: Defenders of air, space and cyberspace, January 28, 2018.
[20] Interview with Maj Dee Randolph (SAF CIO-A6/A3)
[21] Google Research, BeyondCorp: A New Approach to Enterprise Security, Abstract
[22] Ibid, p 1.
[23] Ibid, p 1.
[24] Mimoso, No Firewalls, no problem for Google, February 15, 2017.
[25] Google Research, BeyondCorp: A New Approach to Enterprise Security, p 6.
[26] Ibid, p 6.
[27] Google Research, BeyondCorp: Design to Deployment at Google, p 30.
[28] Ibid, p 29.
[29] Ibid, p 29.
[30] Google Research, BeyondCorp: A New Approach to Enterprise Security, p 8.
[31] Ibid, p 8.
[32] Ibid, p 8.
[33] Ibid, p 8.
[34] Google Research, BeyondCorp: Design to Deployment at Google, p 31.
[35] Google Research, BeyondCorp: A New Approach to Enterprise Security, p 8.
[36] Google Cloud Platform, Cloud Identity-Aware Proxy Product Sheet.
[37] SAF CIO-A6 Info Dominance Flight Plan, p 27.
[38] Derived from DISA Customer Portal data sheets for each Enterprise Service
[39] DISA IASE website
[40] Interviews with Ms. Teresa Salazar (Joint Staff/J6) and Maj Dee Randolph (SAF CIO-A6/A3)
[41] Interview with Lt Col Dave Nuckles (HAF/A1)
[42] SAF CIO-A6 Info Dominance Flight Plan, p 9.
[43] Google Research, BeyondCorp: A New Approach to Enterprise Security, p 8.
[44] USCYBERCOM Mission Statement

Bibliography

Air Force Personnel Center, *17D Development Team Fall outbrief*, October 2017.

DISA Enterprise Services Portal, accessed 17 March 2018, https://www.disa.mil/Enterprise-Services/Applications/.

DISA Information Assurance Support Environment, accessed 17 March 2018, https://iase.disa.mil/Pages/index.aspx.

DMAG briefing, DoD CAPE, subject: CMF C2 manpower decision, 7 June 2017.

Google Cloud Platform information site, accessed 17 March 2018, https://cloud.google.com/iap/.

Osborn, Barclay, et al., Google Research, ;login, *BeyondCorp Design to Deployment at Google*, Vol 41, No 1, Spring 2016.

Ward, Rory and Beyer, Betsy., Google Research, ;login, *BeyondCorp A New Approach to Enterprise Security*, Vol 39, No 6, December 2014.

Joint Staff J1, Headquarters, United States Cyber Command and JFHQ Manpower Requirements Assessment Reports, 1 November 2016

Joint Staff J6 briefing, CFMITT, subject: CMF Quarterly Build Report, FY18 Q1, December 2017.

Mimoso, Michael., ThreatPost, *No Firewalls, No Problem for Google*, accessed 17 March 2018, https://threatpost.com/no-firewalls-no-problem-for-google/123748/.

Nuckles, David, Lt Col, USAF., HAF/A1, Interview by the author, 5 December 2017.

Randolph, Dee, Maj, USAF., SAF CIO/A3/A6, Interview by the author 6 December 2017.

SAF CIO-A6, *Air Force Information Dominance Flight Plan Operating In, Thru and From Cyberspace*, accessed 17 March 2018, http://www.safcioa6.af.mil/Portals/64/documents/20170203-%20IDFPv3.pdf?ver=2017-02-16-072244-507

Salazar, Teresa, SES, Joint Staff J6, Interview by the author, 6 December 2017.

Skinner, Robert J., Maj Gen, USAF., The Washington Times, America's Air Force: Defenders of air space and cyberspace, accessed 17 March 2018, https://www.washingtontimes.com/news/2018/jan/28/americas-air-force-defenders-of-air-space-and-cybe/.

USCYBERCOM, *Mission Statement*, accessed 17 March 2018, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.

Weggeman, Chris P., Maj Gen, USAF., *Presentation to the Senate Armed Services Committee Subcommittee on Cybersecurity, Subject: Military Cyber Programs and Posture*, 13 March 2018.