2018 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
VEHICLE ELECTRONICS AND ARCHITECTURE (VEA) & GROUND SYSTEMS CYBER ENGINEERING (GSCE) TECHNICAL SESSION
AUGUST 7-9, 2018 – NOVI, MICHIGAN

SECURE WIRELESS ARCHITECTURE FOR GROUND VEHICLES

Charlie Kawasaki, CISSP
CTO
Pacific Star Communications, Inc (dba PacStar)
Detroit, MI

ABSTRACT

US Army and Marine Corps tactical networking and command post programs have a widely-acknowledged critical need to improve mobility, including the objective of moving to mobile, vehicle-mounted command posts that can move hourly. The current state of the art for tent-based command posts requires hours of setup, which includes thousands of feet of copper wiring that delay network availability. To enable mobility for warfighting, the National Security Agency (NSA) established a program (with a set of guidelines) called "Commercial Solutions for Classified" (CSfC). CSfC-based mobility solutions have great potential to enable command post mobility and soldier dismounted situational awareness using ground vehicles as network nodes. However, the extensive requirements and processes involved are complex and not well understood. This paper compares various CSfC network architectures, and proposes several approaches for CSfC solutions optimized for mobility use cases. The paper further describes state of the art technologies suitable for such solutions.

INTRODUCTION

US Army and Marine Corps tactical networking and command post programs have a widely-acknowledged critical need to improve mobility, including the publicly stated objective of moving to mobile, vehicle-mounted command posts that can move hourly. The current state of the art for tent-based command posts requires hours of setup, which includes thousands of feet of copper wiring that delay network availability, resulting in a dangerous lack of situational awareness for commanders.

To enable mobility for warfighting, the National Security Agency (NSA) established a program (with a set of guidelines) called "Commercial Solutions for Classified" (CSfC)[1]. This program enables DoD organizations to transmit classified information using commercial-grade encryption solutions, eliminating the need for expensive, difficult-to-use classified equipment.

CSfC enables access to classified information using inexpensive, commercial technologies, providing benefits such as:

- Enabling entirely new classes of wireless access to classified networks for warfighting
- Enabling US coalition partners to access classified information without taking possession of controlled cryptographic items (CCI)
- Significantly reduces equipment costs and simplifies key management
- Simplifies equipment handling/security procedures

CSfC-based communications solutions transmit classified information via two layers of commercial encryption solutions. Previously, the only means to transmit classified information was via expensive, controlled, military grade encryption devices such as SECNET-54s and KG-250s.

CSfC-based mobility and wireless solutions have great potential to enable command post mobility and soldier-dismounted situational awareness using ground vehicles as radio nodes. Research and design for such use cases are under way. However, to meet CSfC and DoD requirements for classified networking, systems integrators and technology developers must follow extensive sets of requirements and processes that are both complex and not well-understood.

This paper describes, compares and contrasts various CSfC network architectures, and proposes several approaches for CSfC solutions optimized for tactical networks and mobility use cases.

INTRODUCTION TO CSFC ARCHITECTURE AND PROCESS

The diagram below demonstrates how classified information can be transmitted over untrusted wireless connections such as Wi-Fi, LTE, and SATCOM, including public, government and partner networks. This is achieved by using two sets of encryption technologies, one layered inside the other. Approved configurations include encryption using VPN inside VPN, VPN inside Wi-Fi WPA2, MACsec inside VPN, and TLS inside VPN.

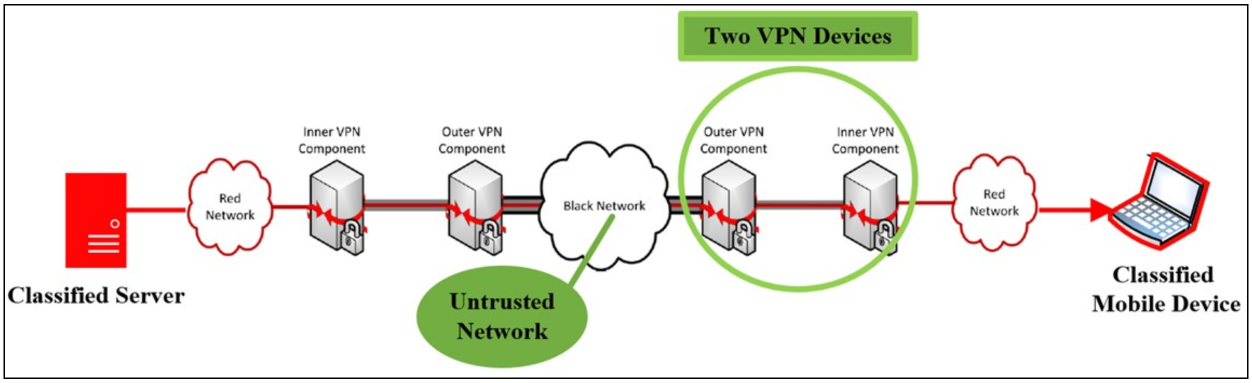

Figure 1: Simplified CSfC Architecture

Though layered encryption is straightforward in concept, full CSfC implementations must include a breadth of technologies, including public key infrastructure, encryption gateways and clients, authentication systems, cybersecurity technologies, and secure network infrastructure. Additionally, to successfully field systems, the

CSfC program requires organizations to follow a well-defined process. An overview of the technologies and processes is shown below.

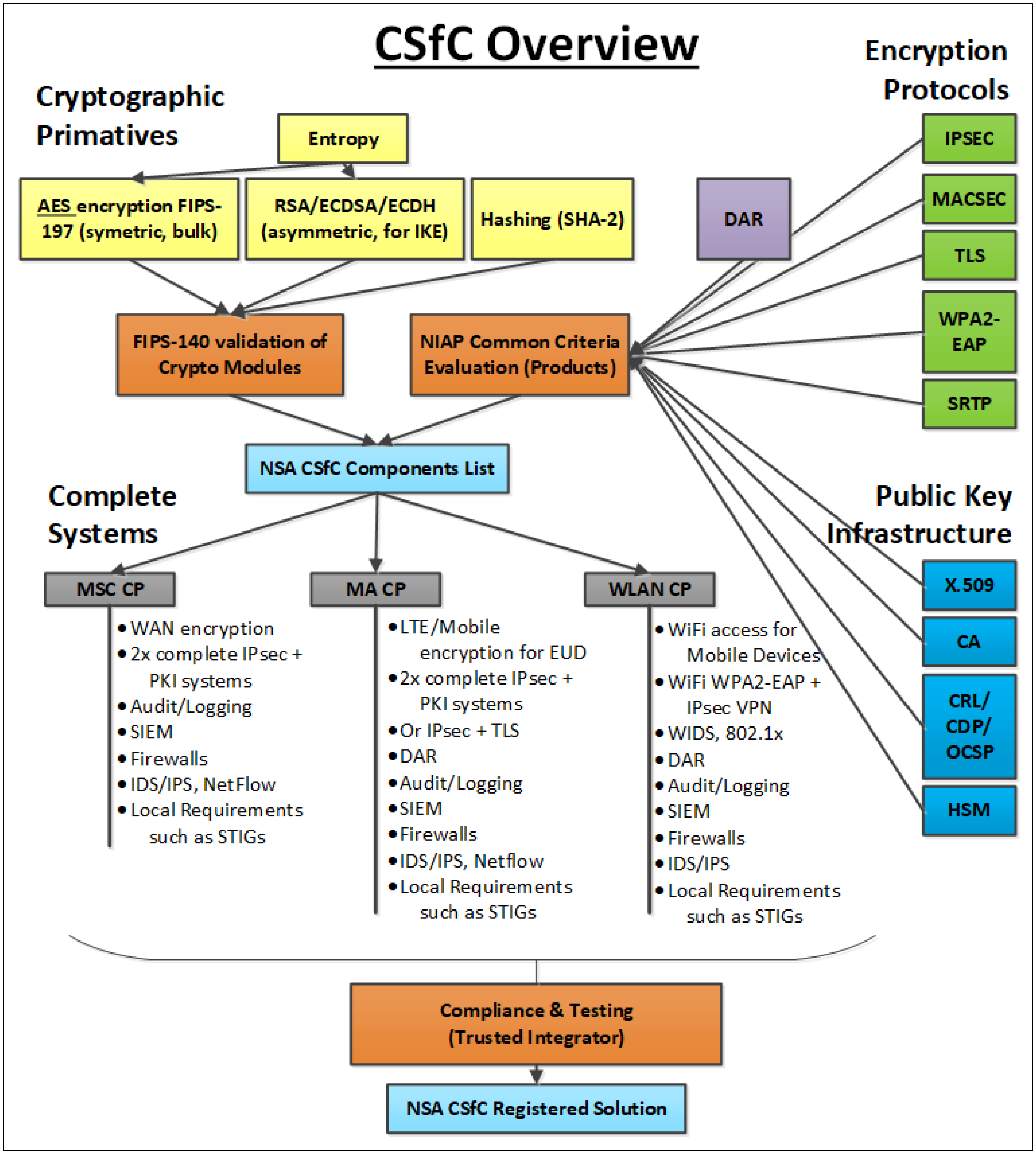
CSfC Overview
Cryptographic Primatives
Entropy
AES encryption FIPS-197 (symetric, bulk)
RSA/ECDSA/ECDH (asymmetric, for IKE)
Hashing (SHA-2)
DAR
Encryption Protocols
IPSEC
MACSEC
TLS
WPA2-EAP
SRTP
FIPS-140 validation of Crypto Modules
NIAP Common Criteria Evaluation (Products)
NSA CSfC Components List
Complete Systems
Public Key Infrastructure
X.509
CA
CRL/ CDP/ OCSP
HSM
MSC CP
• WAN encryption
• 2x complete IPsec + PKI systems
• Audit/Logging
• SIEM
• Firewalls
• IDS/IPS, NetFlow
• Local Requirements such as STIGs
MA CP
• LTE/Mobile encryption for EUD
• 2x complete IPsec + PKI systems
• Or IPsec + TLS
• DAR
• Audit/Logging
• SIEM
• Firewalls
• IDS/IPS, Netflow
• Local Requirements such as STIGs
WLAN CP
• WiFi access for Mobile Devices
• WiFi WPA2-EAP + IPsec VPN
• WIDS, 802.1x
• DAR
• Audit/Logging
• SIEM
• Firewalls
• IDS/IPS
• Local Requirements such as STIGs
Compliance & Testing (Trusted Integrator)
NSA CSfC Registered Solution

Figure 2: OV-1 CSfC Technologies, Components, Solutions and Process

The overview above includes the following major CSfC-related technology and process components:

- Shown in yellow, the “Cryptographic Primitives” are the approved algorithms and mathematics that the NSA specifies for transmission of classified information.
- Shown in green, the “Encryption Protocols” are approved to conduct communications between devices that transmit encrypted data. Most used today are VPN solutions providing data-in-transit encryption.
- Shown in purple is “DAR” (Data-at-Rest) encryption technology. This type of technology is used to encrypt data stored on media such as hard drives, flash drives, etc.
- Shown in blue is “Public Key Infrastructure”, the approved technologies and protocols required to manage trust, encryption key generation, and sharing.
- Shown in brown are key validation and testing processes required by the CSfC program in order to comply with CSfC rules.
- Shown in small gray boxes are the main NSA CSfC “Capability Packages” (CPs)[2] specifying the architecture, component and technical requirements, testing and personnel roles that must be documented and followed.
- Shown in light blue are the two major “approval” statuses of technologies. The first is a listing of approved commercial (OEM) components that may be included in solutions. The second and final light blue box shows a completed solution, approved by the CSfC program and ready for deployment.

Organizations can select from the technologies above to create integrated solutions that enable classified networking over radio infrastructure such as SATCOM, Wi-Fi, LTE or LMR, enabling vehicles to communicate with upper echelons/HQ, or enabling soldiers to use mobile devices such as laptops, tablets or smartphones, in transit, at the halt, and in dismounted use cases. In the sections that follow, a number of architectures are described that follow NSA CSfC “Capability Packages”, and are designed to enable these use cases.

DETAILED CSFC ARCHITECTURES

There are several main CSfC architectures approved by NSA for transmitting classified information over Wide Area Networks (WAN) and Wireless Local Area Network (WLAN) infrastructure, depending on the desired use cases. These architectures are specified in NSA “Capability Packages”, which outline in great detail the components, configurations, processes, and testing required by NSA before they will approve the use of a system.

Of the allowable architectures, the ones below are most suited for use by ground vehicles for both WAN communications with upper echelons/HQ or teleport sites, and WLAN communications for short-range communications with end-user devices.

Multi-site Connectivity Capability Package

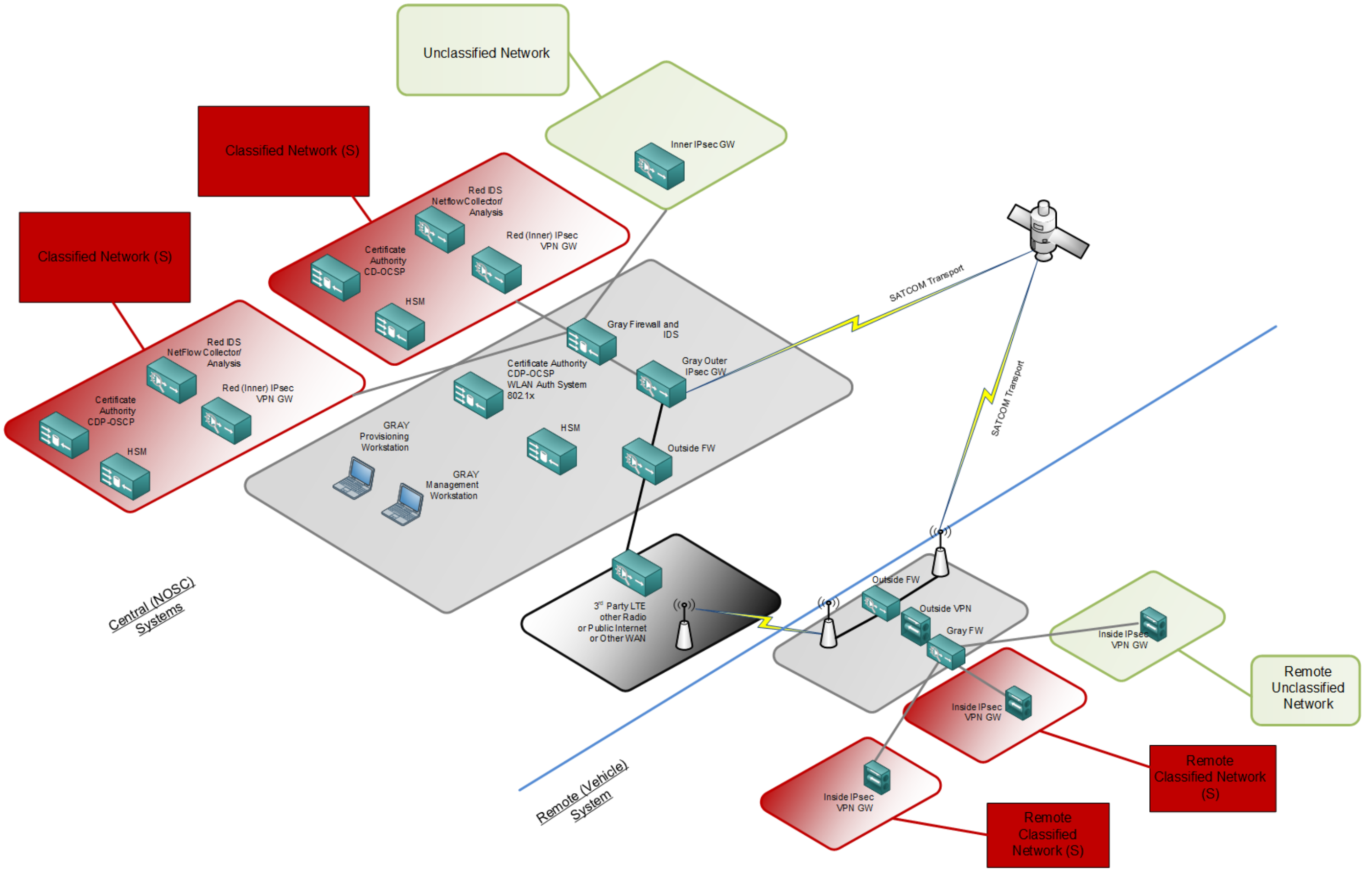

Figure 3: WAN Encryption using Dual VPN MSC CP

This configuration shows the ability to utilize any type of wireless transport for network WAN access, including SATCOM, Wi-Fi, LTE or other radio types so that deployed, remote CSfC gateways may include a minimum of deployed equipment. This architecture follows the NSA Multi-Site Connectivity Package v1.0 Access Capability Package[3], with a Central Management Site (NOSC) and a Remotely Managed Site, utilizing two layers of IPsec VPN encryption. In the case of ground vehicles, the Remote System could be vehicle mounted, and, depending on the number and type of networks being accessed, as well as bandwidth requirements, the Remote System could comprise just two small vehicle-mounted VPN gateways.

This architecture includes (Remote Equipment):

- An optional, single outside firewall. This architecture uses one of these units per vehicle, but is only required when using non-government-owned radios or "public internet".
- A single, outer IPsec VPN gateway, used to establish an outside VPN tunnel. This device establishes the first layer of VPN encryption for remote users, meeting CSfC requirements. This architecture uses ONE of these units per vehicle.
- A Gray firewall. This module is only required if the vehicle needs access to multiple classified networks of different levels of classification. To provide access to only a single classified network, this module may be dropped.
- An inside IPsec VPN gateway. This module provides the second layer of VPN encryption, as required by CSfC. This architecture uses ONE of these units per remote network.

This architecture includes Central-side NOSC equipment, which would typically reside at an upper echelon, STEP site, or command post. The architecture includes:

- A Gray outside firewall, only required if the radio infrastructure is considered "public internet", and not owned by US Government.
- Gray outside IPsec VPN termination gateway
- Gray firewall
- Management services including Certificate Authority, Authentication, and Gray Security Incident and Event Manager (SIEM).
- Each network at the NOSC Red enclaves must each contain an inner IPsec VPN gateway.
- Red enclaves may include management services, including a Certificate Authority (CA), SIEM, IDS, and NetFlow collector, if the Red network does not include enterprise CA and cybersecurity tools.

Campus WLAN Capability Package

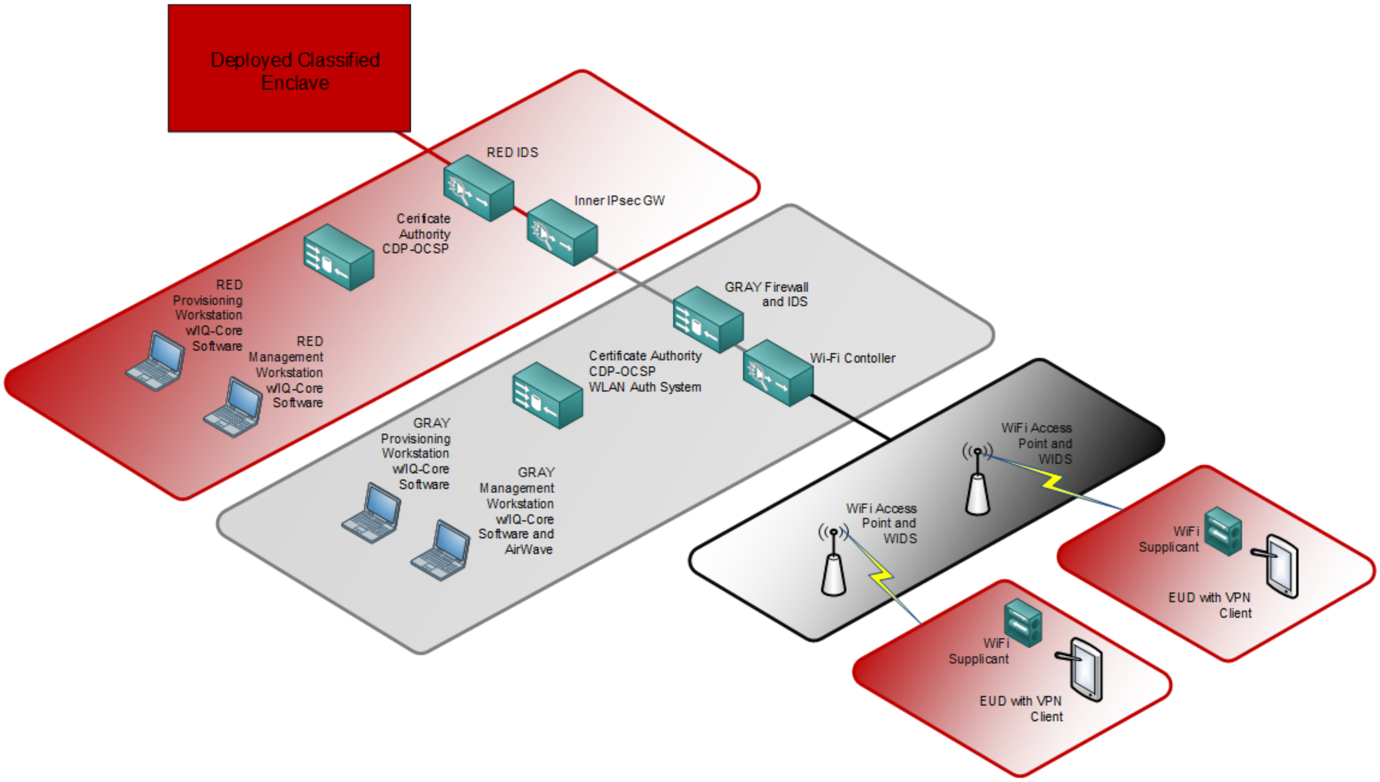
Deployed Classified Enclave
RED IDS
Inner IPsec GW
Cerificate Authority CDP-OCSP
RED Provisioning Workstation w/IQ-Core Software
RED Management Workstation w/IQ-Core Software
GRAY Firewall and IDS
Wi-Fi Contoller
Certificate Authority CDP-OCSP WLAN Auth System
GRAY Provisioning Workstation w/IQ-Core Software
GRAY Management Workstation w/IQ-Core Software and AirWave
WiFi Access Point and WIDS
WiFi Access Point and WIDS
WiFi Supplicant
EUD with VPN Client
WiFi Supplicant
EUD with VPN Client

Figure 4: WLAN Encryption using Wi-Fi WLAN CP

For organizations looking to develop vehicle-mounted, classified WLAN systems that can enable on the move and dismounted Situational Awareness (SA) over short distances, the NSA Campus WLAN Capability Package v2.0[4] architecture is an option. The architecture above assumes a pre-existing WAN encryption solution, and adds the deployment of vehicle-mounted Wi-Fi so that End-User Devices (EUDs) can be deployed on a wireless LAN with access to classified information.

This architecture uses the Campus WLAN Capability Package v2.0, utilizing built-in commercial Wi-Fi stack (supplicant) and OS security on the EUD to provide one layer of the required two-layer package. The architecture uses a single IPsec VPN client on the EUD to provide the second, inner encryption layer. This architecture provides for a straightforward EUD configuration using well-tested approaches.

This architecture includes the following mobile EUD configuration:

- Laptop-based Wi-Fi drivers and OS encryption (using WPA2, EAP-TLS and 802.1x) terminating the Wi-Fi security layer.
- VPN client running on wireless user laptops. This VPN client terminates at the inner VPN gateway on the RED network.

This architecture also includes the following vehicle-mounted, central configuration:

- Wi-Fi/Mobility Controller, used to manage the local Wi-Fi networks. This device establishes the second (outside) layer of Wi-Fi encryption for EUDs, which is essential to meeting CSfC requirements. It also provides Wireless Intrusion Detection Sensor (WIDS) capabilities.
- Lightweight access points for networking, which provide WLAN radio services. In this architecture, Wi-Fi encryption is not performed on the Access Points (APs), but on the controller.
- Vehicle-mounted SIEM, Authentication Server, Certificate Authority, Firewalls, and WIDS controller.

Mobile Access Capability Package with VPN EUD

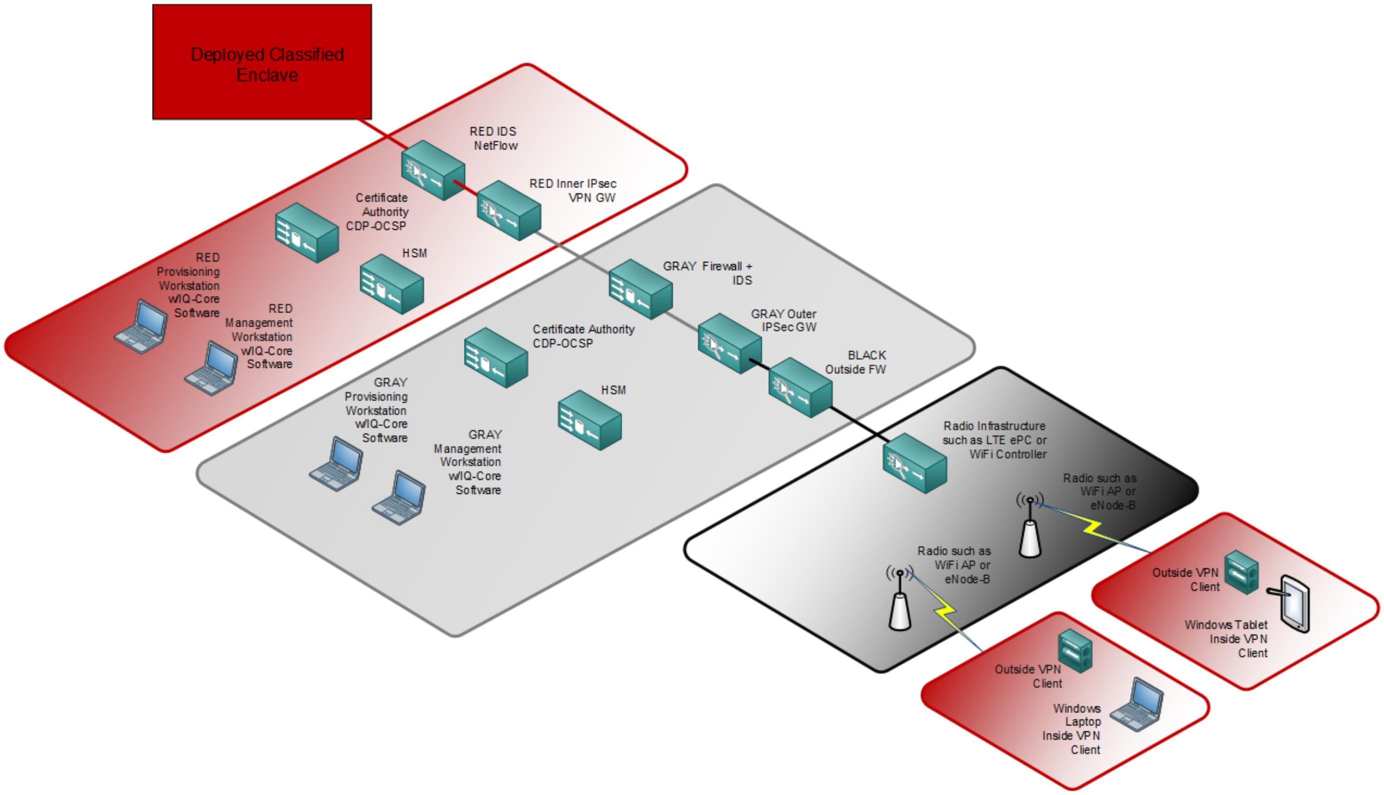
Deployed Classified Enclave
RED IDS NetFlow
RED Inner IPsec VPN GW
Certificate Authority CDP-OCSP
HSM
RED Provisioning Workstation w/IQ-Core Software
RED Management Workstation w/IQ-Core Software
GRAY Firewall + IDS
GRAY Outer IPSec GW
BLACK Outside FW
Certificate Authority CDP-OCSP
HSM
GRAY Provisioning Workstation w/IQ-Core Software
GRAY Management Workstation w/IQ-Core Software
Radio Infrastructure such as LTE ePC or WiFi Controller
Radio such as WiFi AP or eNode-B
Radio such as WiFi AP or eNode-B
Outside VPN Client
Windows Tablet Inside VPN Client
Outside VPN Client
Windows Laptop Inside VPN Client

Figure 5: WLAN Encryption using any radio via MA CP VPN EUD

For organizations looking to develop vehicle-mounted, classified WLAN systems the NSA Mobile Access Capability Package v2.0[5] is an option. WLAN can enable on the move and dismounted SA over distances longer than Wi-Fi radios can support. The architecture above assumes a pre-existing WAN encryption solution, and adds the deployment of vehicle-mounted radios (of any type) so EUDs can be deployed on a wireless LAN with access to classified information at longer distances. Rather than depending on the Wi-Fi supplicant on EUDs, this architecture requires two layers of VPN encryption, and is radio/transport-independent.

This architecture includes the following mobile EUD configuration:

- Inner VPN client running on wireless user laptops. This VPN client terminates at an inner VPN gateway.
- Outer VPN client running on wireless user laptops. This VPN client terminates at the outer VPN gateway.
- These VPN clients must be hypervisor separated on the EUD.

This architecture also includes the following vehicle mounted, central, configuration:

- Outer VPN gateway. This device establishes the second (outside) layer of IPsec VPN encryption for EUDs, which is essential to meeting CSfC requirements.
- Inner VPN gateway. This module provides the second layer of VPN encryption, as required by CSfC.
- Vehicle-mounted SIEM, Authentication Server, Certificate Authority, Firewalls, and WIDS controller.
- Any black wireless transport, including Wi-Fi, LTE, or LMR.

This architecture allows multiple simultaneous wireless transports to be supported without additional changes in the encryption scheme. Transports could include Wi-Fi, cellular and IP over LMR (Land Mobile Radio). Additionally, multiple security domains could share those transports with the addition of CSfC-approved components.

Mobile Access Capability Package with TLS EUD

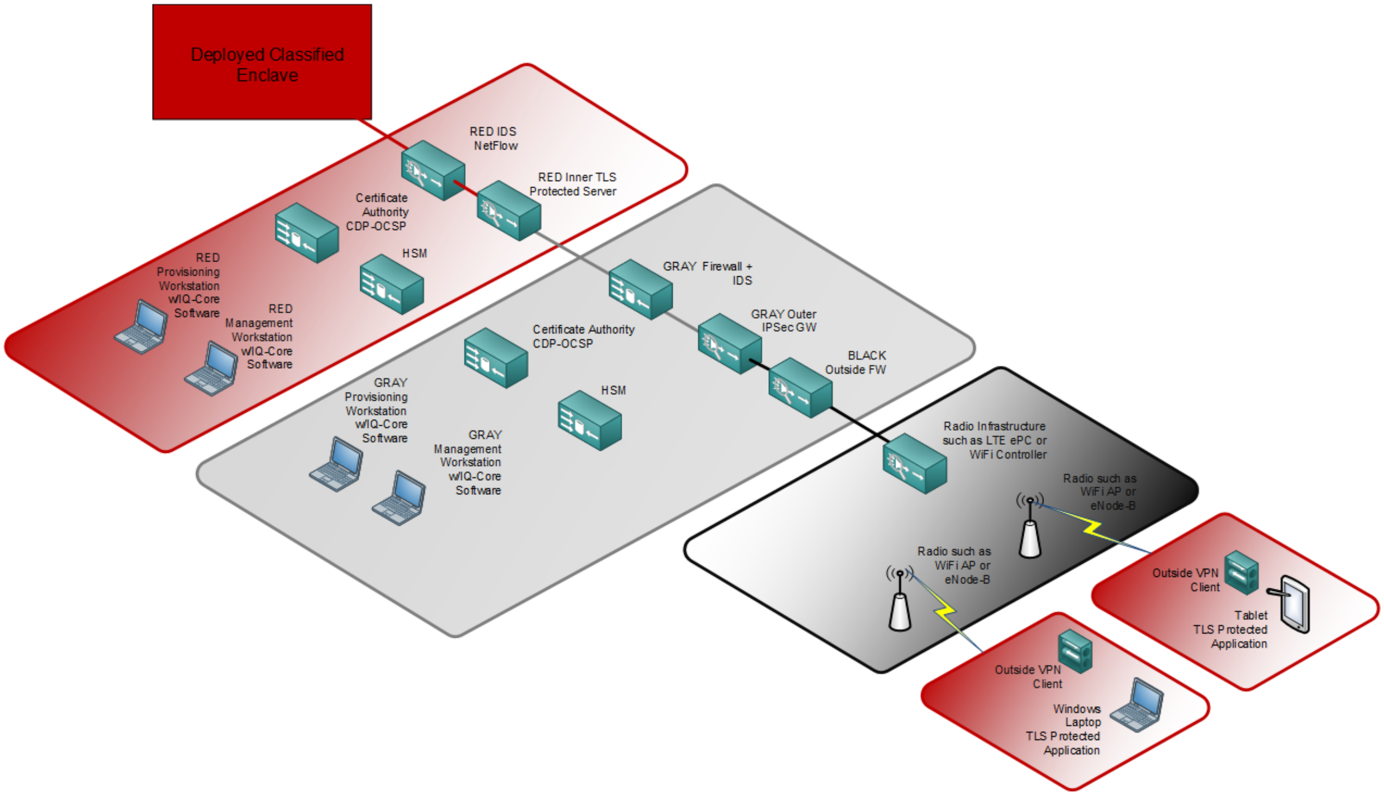
Deployed Classified Enclave
RED IDS NetFlow
RED Inner TLS Protected Server
Certificate Authority CDP-OCSP
HSM
RED Provisioning Workstation w/IQ-Core Software
RED Management Workstation w/IQ-Core Software
GRAY Firewall + IDS
GRAY Outer IPSec GW
Certificate Authority CDP-OCSP
HSM
GRAY Provisioning Workstation w/IQ-Core Software
GRAY Management Workstation w/IQ-Core Software
BLACK Outside FW
Radio Infrastructure such as LTE ePC or WiFi Controller
Radio such as WiFi AP or eNode-B
Radio such as WiFi AP or eNode-B
Outside VPN Client
Tablet TLS Protected Application
Outside VPN Client
Windows Laptop TLS Protected Application

Figure 6: WLAN Encryption using any radio via MA CP TLS EUD

For organizations looking to deploy a vehicle-mounted, classified WLAN for use cases similar to the Mobile Access Capability Package (MA CP) VPN EUD above, but wishing to overcome hypervisor separation requirements, using the TLS-EUD architecture is an option. This architecture follows the NSA Mobile Access Capability Package v2.0 utilizing one layer of VPN encryption (outside) and a second layer of TLS and/or SRTP (Secure Real-time Transport Protocol) (inside) to provide select voice and data access to mobile devices over wireless infrastructure. This architecture is referred to as MA CP TLS-EUD for TLS encrypted EUD access.

This architecture is similar to the MA CP VPN EUD described above, but replaces the inner layer of encryption with a TLS-encrypted server for the inner encryption component, and a TLS-encrypted application on the client EUD.

TECHNOLOGY SELECTION AND DEPLOYMENT CONSIDERATIONS

While systems following the CSfC program can transform communications for the soldier by enabling classified networking over wireless infrastructure, they have two significant issues: size and complexity. The CSfC program requires that solutions include comprehensive suites of security technologies at the command post or datacenter, and the CSfC program mandates that the technologies be provided by different vendors. With the number of required components in CSfC systems, vehicle integration can be a challenge due to the size, weight, and power limitations imposed by vehicles. The diversity of equipment also creates a system configuration, management and training burden that many organizations are underequipped to manage. The following sections address methods to mitigate these challenges.

Size, Weight and Power

True mobility demands innovation and modernization designed to reduce size, weight, and power (SWaP) requirements. Not only do dismounted soldiers need mobility, but so does the network infrastructure to support them – when central-side NOSC equipment is vehicle-mounted.

All else being equal, communications equipment can never be too small, too light, or too power-efficient. In contrast to legacy, data-center style 19” rack mount equipment, new generations of equipment designed for tactical/expeditionary use are becoming available for use with CSfC-capable technologies. Additionally, with network function virtualization, many CSfC-required technologies may be co-located on a single server platform, such as the one shown below.

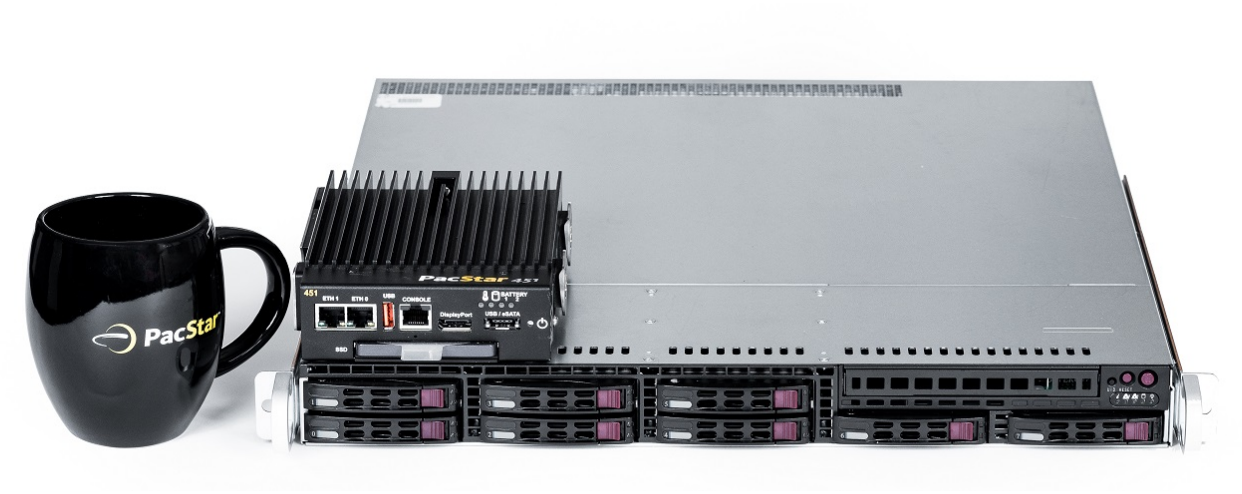

Figure 7: Illustration of SWaP savings from tactical equipment vs. 19” rack mount legacy gear

For example, new tactical equipment, as compared to legacy 19” rack mount equipment on average:

- Is 10.4 times lighter than a typical 1ru server
- Is 12.4 times smaller than a typical 1ru server
- Consumes up to 18 times less power

These types of low SWaP solutions enable maximum program flexibility, enabling vehicle-mounted, roll-on/roll-off, fly away, and stationary use cases, all using the same hardware platform.

Ruggedization and Environmental Testing

To ensure reliable uptime of CSfC-based solutions in vehicle mount applications, components should be selected that have completed and passed a suite of MIL-STD testing appropriate for vehicle-mounted use cases, including for environment, EMI and power, including MIL-STD-810G, MIL-STD-461F and MIL-STD-704D. These tests should have been conducted by independent, outside laboratories, and, where applicable, with the equipment powered on and operating.

Some manufacturers may cut corners on tests, test to a subset of these standards, or simply claim products are “designed for MIL-STD 810”. The end result of reliable validation/verification testing for systems is a complete set of reports detailing every test across a broad range of environmental criteria.

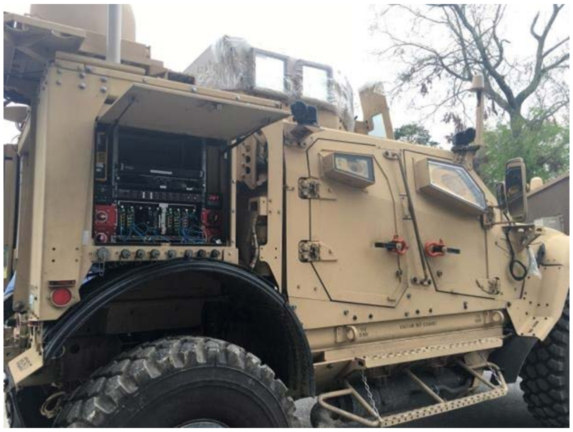

Figure 8: Rugged Communications Equipment Mounted on Marine Corp JLTV[6]

Organizations should consider solutions that have undergone at least:

- 18 types of MIL-STD-810G environmental tests, including vibration in a variety of vehicles (ground, helicopter, etc), shock, crash safety, high/low temperature, humidity, altitude, acceleration, blowing sand/dust, and explosive atmosphere – at the component and chassis level.
- 7 types of MIL-STD-461F EMI tests, including radiated emissions, radiated susceptibility, conducted emissions, conducted susceptibility – at the entire solution level.
- 5 types of MIL-STD-704D power quality tests, including DC Load, Voltage Limits, Voltage Transients, Abnormal DC and Emergency Operation DC.

PACKAGING

NSA continues to evolve CSfC guidelines, frequently adding requirements as threats evolve and technology improves. Organizations looking to deploy CSfC solutions should consider modular systems that are flexible and easily upgradeable, avoiding costly fork-lift replacements, supply chain and logistical rework.

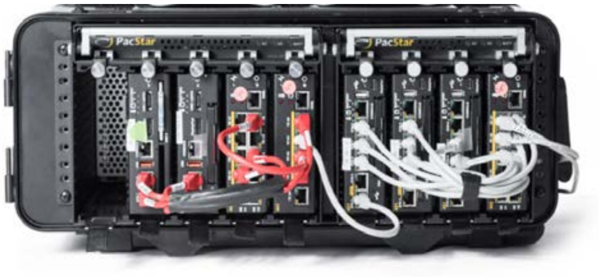

Figure 9: Modular, Tool-less, Dockable, Dismountable Chassis with Built-in UPS.[7]

There are module options available today that address this need through modular design, including vehicular rack mount solutions. Some solutions include the ability to replace modules without requiring tools. Some systems include completely dismountable solutions, with a built-in UPS.

Configuration Management and Monitoring

To address the added complexity and training burden imposed by the two layers of encryption and extensive security requirements, organizations should consider CSfC-specific configuration management tools. These tools can simplify the setup, configuration, and management of the underlying equipment and devices used in CSfC solutions.

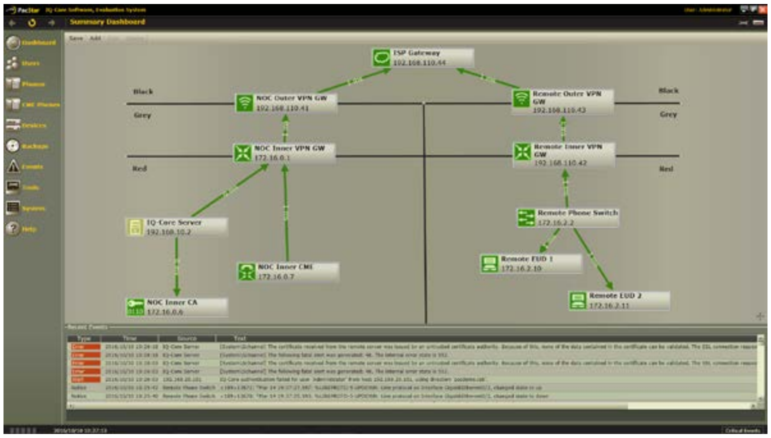
PacStar
Summary Dashboard
Dashboard
Save
Add
ISP Gateway 192.168.110.44
Black
Grey
Red
NOC Outer VPN GW 192.168.110.41
Remote Outer VPN GW 192.168.110.43
NOC Inner VPN GW 172.16.0.1
Remote Inner VPN GW 192.168.110.42
IQ-Core Server 192.168.10.2
NOC Inner CMI 172.16.0.7
NOC Inner CA 172.16.0.6
Remote Phone Switch 172.16.2.2
Remote EUD 1 172.16.2.10
Remote EUD 2 172.16.2.11
Black
Grey
Red
Recent Events
Type
Time
Source
Text

Figure 10: Integrated Configuration Management/Monitoring Software with CSfC-Specific Capabilities [8]

Such tools can provide a base level of capabilities, including:

- Enabling the deployment of CSfC solutions, with attendant benefits, while reducing the amount of added complexity and training
- Providing a unified interface ("a single pane of glass") to underlying equipment from multiple vendors
- Providing a means to monitor multiple sets of equipment, in fixed/branch offices and tactical settings, enabling lightly trained operators to manage the equipment

Organizations should consider functionality specifically designed to make CSfC manageable, including:

VPN Setup Wizards

VPN setup and certificate generation wizards reduce the complexity of providing the correct information to the devices involved in CSfC encryption by providing step-by-step wizards, insulating lightly-trained users from dealing with the command line interfaces and multiple UIs across the underlying devices.

VPN Monitoring/Troubleshooting

VPN monitoring capabilities include the ability to display, in real time, the connection and configuration status of one or more VPN devices. Status indicators should include status of the active authentication and bulk encryption settings in use, ensuring the connection is compliant with CSfC guidelines.

Certificate Management

Management capabilities include automating the process of managing device certificates, a process that is error-prone, and requires extensive training. Reducing the opportunity for errors in this process helps ensure communications uptime and allows security administrators to focus on more important tasks. Capabilities related to certificates should include:

- Generation of certificate signing requests
- Display of certificate details and expiration dates, including expiration alerts
- Encrypted transmission of certificate signing requests
- Management of the signing process at either the deployed systems or at the NOSC
- Management/monitoring of certificate authorities
- Providing certificate revocation checking via built-in OCSP and CDP functions.

By using management tools such as the software platform described above, the US Army is deploying CSfC solutions and gaining the benefits of WiFi in tactical settings, reducing command post setup time and enabling new classes of wireless applications, while limiting management complexity and training burdens.

An independent Human Factors Engineering analysis of one such tool found dramatic savings for entry-level and advanced administrators in time savings and reduction in errors, when using it for CSfC and general network administration-related tasks.

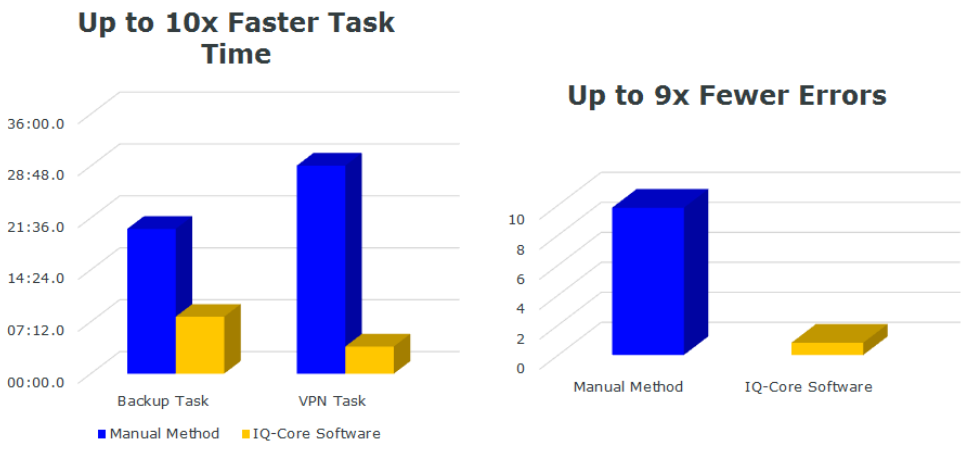

Figure 11: Dramatic savings in time and errors via integrated management software [9]

REFERENCES

[1] Commercial Solutions for Classified Program (CSfC). April 16, 2018. NSA; [accessed 2018 May 30]. https://www.nsa.gov/resources/everyone/csfc/

[2] Commercial Solutions for Classified Program (CSfC), Capabilities Packages. April 16, 2018. NSA; [accessed 2018 May 30]. https://www.nsa.gov/resources/everyone/csfc/capability-packages/

[3] Commercial Solutions for Classified Program (CSfC), Multi-Site Connectivity Capability Package. April 16, 2018. NSA; [accessed 2018 May 30]. https://www.nsa.gov/resources/everyone/csfc/capability-packages/#multi-site

[4] Commercial Solutions for Classified Program (CSfC), Campus WLAN Capability Package. April 16, 2018. NSA; [accessed 2018 May 30]. https://www.nsa.gov/resources/everyone/csfc/capability-packages/#wlan

[5] Commercial Solutions for Classified Program (CSfC), Mobile Access Capability Package. April 16, 2018. NSA; [accessed 2018 May 30]. https://www.nsa.gov/resources/everyone/csfc/capability-packages/#mobile-access

[6] PacStar Awarded $10 Million US Marine Corps Networking On-The-Move (NOTM) Contract. September 12, 2017 PacStar. [accessed 2018 May 30] https://pacstar.com/pacstar-awarded-10-million-us-marine-corps-networking-on-the-move-notm-contract/

[7] PacStar Secure Wireless Command Post (Wi-Fi) c2018. [accessed 2018 May 30] PacStar. https://pacstar.com/products/csfc/pacstar-secure-wireless-command-post-wi-fi/

[8] U.S. Army Deploys PacStar IQ-Core® Software Across WIN-T Increment 1 Network. October 3rd 2016. PacStar. [accessed 2018 May 30] https://pacstar.com/u-s-army-deploys-pacstar-iq-core-software-across-win-t-increment-1-network/

[9] Warfighters Configure and Manage Tactical Communications Systems 10x Faster With 9x Fewer Errors Using PacStar® IQ-Core® Software. January 18th 2017. PacStar. [accessed 2018 May 30] https://pacstar.com/warfighters-configure-and-manage-tactical-communications-systems-10x-faster-with-9x-fewer-errors-using-pacstar-iq-core-software/