Developing a Framework To Improve Critical Infrastructure Cybersecurity

145 South 79th Street, Suite 23 Chandler, AZ 85226

1. Executive Summary

Cummings Engineering is pleased to provide these comments in response to the Request for Information by the National Institute for Standards and Technology titled Developing a Framework To Improve Critical Infrastructure Cybersecurity. Cummings Engineering, a privately owned corporation in Chandler, AZ, has provided cybersecurity solutions to the federal government since 2007. Cummings, in coordination with our partner, CACI, has offered Specific Industry Practices.

This submission includes Cummings Engineering, Inc. SAIFE®-branded solutions distributed by Saife Technologies LLC as managed by CACI for our Department of Defense clients. The Practices described enable NIST to enact policies and guidelines that utilize platform-independent and transport-independent applications with ease of use, scalability, and trust in their security. The resulting value is the ability to robustly and securely connect and protect data across disparate network service providers, disparate devices, and disparate infrastructures with a high integrity security chain.

Resulting capabilities include last tactical mile applications, biometric intelligence, multi-level secure environments and various cross-domain applications, and finally applications for the discreet user where anonymity and obfuscation are concerns.

The primary benefits of the featured SAIFE® enterprise secure mobility architecture & solutions described herein include the following:

- **Uses existing network infrastructures. Any network. Any Device - SECURE**

  SAIFE® represents a device agnostic, network agnostic, peer-to-peer security platform for the transmission and or storage of digital information (text, email, voice or any digital data).

  Cost savings are realized since there is no need to buy new devices or modify legacy systems. The use of any device also provides the flexibility to take advantage of BYOD equipment without compromising the personal security of the individual.

- **Integrates with any MDM for client flexibility.**

  “First-of-its Kind” secure architectural framework (SAIFE®) that can be easily integrated with any MDM of the customer’s choice

  SAIFE(R) solutions compliment the MDM by providing the mandatory underpinning of security, agility and guaranteed protection from compromise while the MDM focuses on full device management features and benefits.

- **Uses current government approved certifications (NSA Suite B Security and FIPS 140-2 validated security) for any MDM.**

  Integration by any MDM with SAIFE® provides full FIPS 140-2 compliance. This gives the client flexibility of MDM choice. On July 26th, 2012 the National Institute of Science and Technology (NIST) issued Certificate No. 1759 for Cummings Engineering's Suite Mobility Suite B Crypto Module, v1.0 by Cummings Engineering Consultants, Inc.

Phyllis E Johnson, Vice President, phyllis.johnson@saifetech.com, Phone: 703 282-2039

Cummings Engineering, 145 S. 79th St., Suite 26, Chandler, Arizona 85226

Phone: 480-809-6020, Fax: (480) 809-6021)

Table of Contents

2. Industry Best Practices

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

• Mission/system resiliency practices;

• Security engineering practices

• Use of encryption and key management;

2.1. Mission/System Resiliency Practices

Our DoD clients use SAIFE® solutions as a next-generation Security-as-a-Service Framework. Solutions are delivered as software-only or cloud modules to adapt into existing infrastructure and minimize costs associated with new IT and on-going management. This removes the requirement for more infrastructure and confined ecosystems. Therefore, it maximizes interoperability between presently disparate ecosystems.

This capability means that the only limitation to the number of users is the limitation of the existing network and communications infrastructure currently in place with the client. Numerous DoD clients have invested millions in their current ability to scale to large numbers of users. These agencies see greater returns and greater functionality with the use of SAIFE solutions.

Platform Design for Increased Scalability

All solutions described herein are built on a common platform, namely the Secure Agile Interoperable Framework for the Enterprise (SAIFE®). A few high-level key advantages of SAIFE® are as follows:

- Delivers the ability to incorporate COMSEC across both legacy and modern devices
- Creates the ability to unify communications between legacy communications and commercial technologies such as smartphones, tablets, etc.
  - Provides application developers ability to quickly add holistic security while enabling interoperability among third-party application providers
  - Simplifies the communications schema
    - Seamlessly sustain communications during transition points (i.e. urban to austere OR pre-op to operational engagement)
- Contains Cost
  - Extends legacy product lifecycle
  - Reduced cost of managing (e.g. Over the Air updates)
  - Exchange cryptographic libraries without disruption to the security target
  - Remove program overruns by incorporating COMSEC into legacy devices

The system overview picture below shows the high-level world-wide secure communication solution enabling any device, any network to establish trusted sessions on-demand in a managed, authenticated fashion.

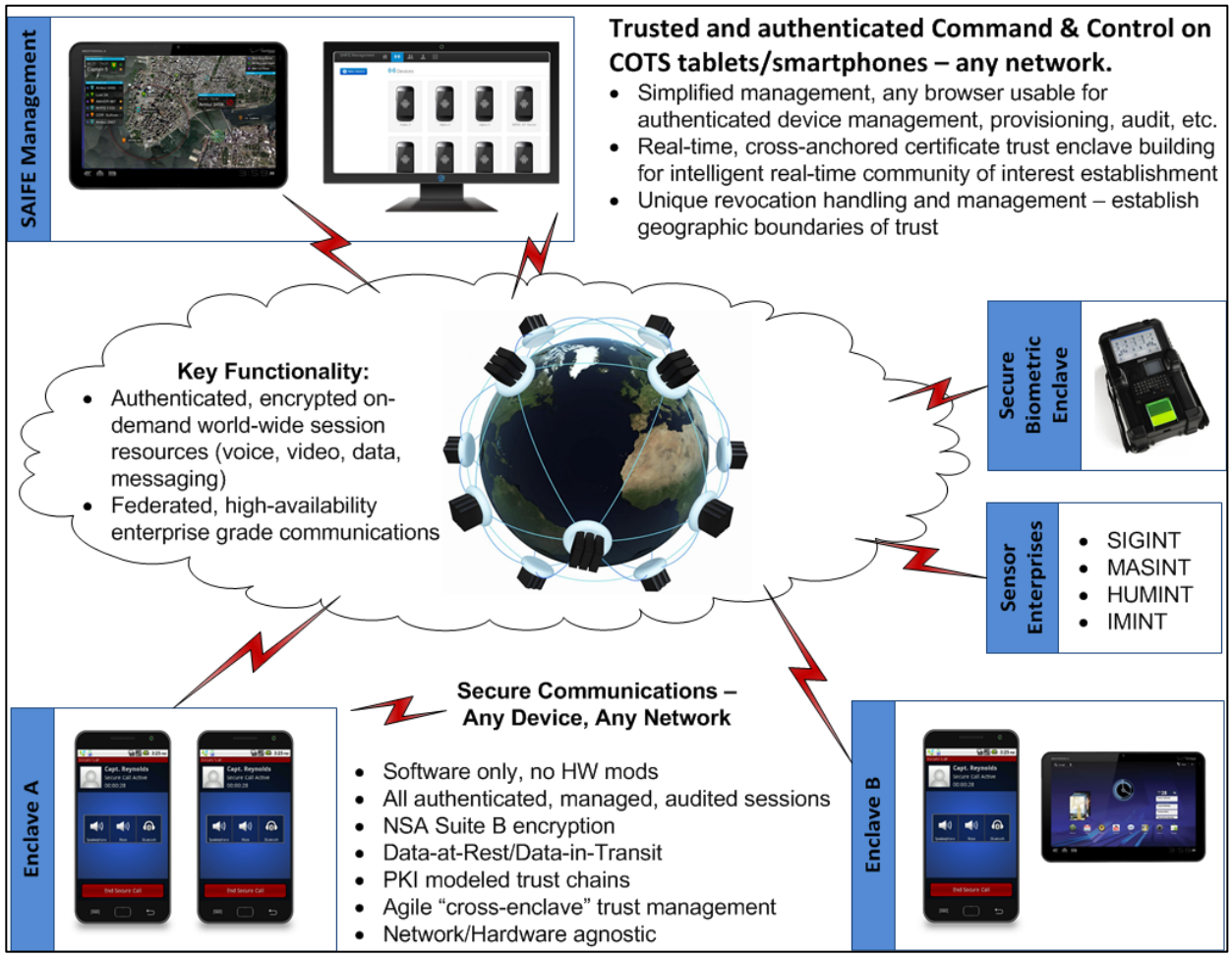

Figure 1 – System Overview of Secure Mobility Solution, Powered by SAIFE

2.2 Security Engineering Practices

The solution is delivered as a cloud-based solution but can be provided as a hybrid "TIPRNET-On-The-Go" whereby the Management occurs through the cloud while the system can operate disconnected with security.

The distinguishing feature of SAIFE®'s unique approach to securing mobile endpoints is its implementation of an all-black (Data is never decrypted during transit; It is only decrypted at the endpoint) cloud-based architecture which provides high-availability and low-latency cryptographic services. The architecture realizes bi-directional store-and-forward services for remote configuration, audit logs, key signing, key revocation, software updates, and other management services. Additionally, the scalable infrastructure allows seamless mobility for SAIFE®-enabled devices allowing these devices to reach protected infrastructure components regardless of intervening network topologies. A SAIFE®-enabled device can transition between geographic regions and disjoint networks without sacrificing security or mobility. SAIFE® offers true robust, seamless mobility.

For the transmission of enterprise-related data, SAIFE®'s Cisco-certified VPN offers a standards-compliant IPsec VPN solution for Android-based devices. Combining the power of SAIFE®'s robust and distributed infrastructure with the scalability and feature-rich Cisco ASA, mobile device data can be delivered securely in an encrypted and authenticated tunnel resulting in a low risk solution for protecting sensitive data. Command, control and configuration data for mobile devices traverses SAIFE®'s all-black, cloud-based network while enterprise-related data traverses the SAIFE® Cisco-certified VPN tunnel to Cisco's ASA to fulfil the critical and necessary role of extending protected infrastructure services to the mobile endpoint.

The framework is currently designed to be a hybrid solution called TIPRNET.

Tactical Internet Protocol Relay Network (TIPRNET™)

One of the US Special Operations Command's current priorities is to expand SOF's capabilities by working with the combatant commands and interagency and allied special-operations partners to establish a global SOF network, which is able to react more rapidly and effectively to enemy action. TIPRNET was built to support the following Mission Priorities of US Special Operations Command, namely:

- Deter, Disrupt, Defeat Terrorist Threats
- Develop & Support our People and Families
- Sustain & Modernize the Force

To realize this goal, agile communication paradigms must be applied. TIPRNET enables the ability to create real-time highly trusted, secure interoperable networks of heterogeneous devices. Smartphones, computers, access points, sensors, etc. can all be cryptographically assured members of an "on-demand" set of assets for the purpose of superior situational awareness and actionable intelligence.

TIPRNET, or the Tactical Internet Protocol Relay Network, is an innovation from Cummings Engineering. It is a realization of the SAIFE framework capability, in software terms it is an instantiation providing secure session services in highly distributed, secure black cloud architecture. The follow are overview distinctions of TIPRNET:

- TIPRNET provides a highly reliable, highly scalable network for low-latency secure session establishment for all data types (voice, video, messaging, etc.).
- TIPRNET uses the SAIFE NSA Suite B cryptography & methodologies on any compatible commodity hardware, allowing for more agility in deployment.
- TIPRNET enables world-wide real-time "communities of interest" across any network

- Overcomes traditional key management issues while leveraging existing PKI technologies and standards (e.g. x.509)
- The SAIFE-endpoint software (e.g. SAIFE® Mobile for secure voice and messaging) installed on each TIPRNET member device (e.g. smartphone) would itself play the role of a Tactical Assurance Internet Protocol Encryptor (TAIPE).
- Each member device accessible through public key credentials

TIPRNET Services

TIPRNET represents a global secure cloud capability providing secure, authenticated, highly reliable network session services. TIPRNET is a collection of internet-based cloud resources creating a secure "sub-net" across an otherwise untrusted network. Security comes through the advantages offered by the SAIFE framework including certificate-driven authentication through a PKI-modelled trust chain ultimately tied to a Certificate Authority. All traffic in the TIRPNET is signed, authenticated and encrypted in a black architecture. Addition features TIPRNET includes a few core SAIFE Technologies including Continuum Services and a Black Connection Gateway Service. The follow outline some of the key distinctions:

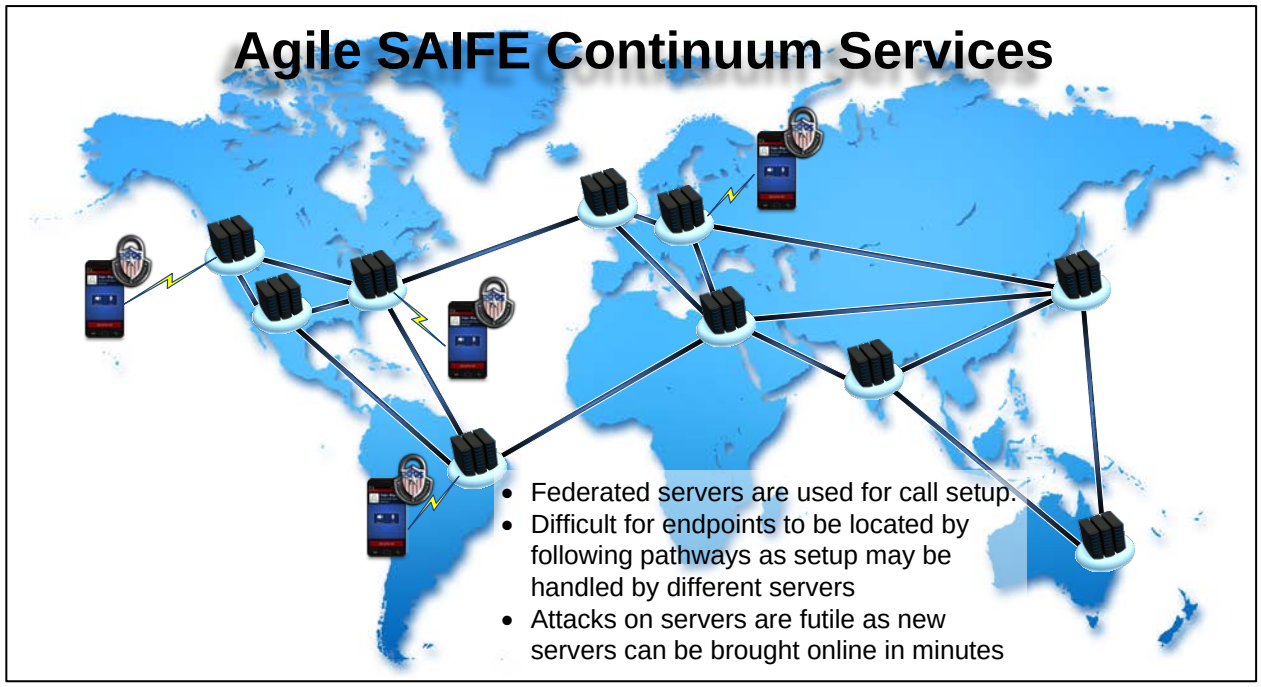

Figure 2 – Agile call setup and robust worldwide TIPRNET™ Services

- Provide high availability, resilient secure session services
- Replace traditional, vulnerable application servers that coordinate sessions:
  - SIP call manager
  - Traditional chat servers
- Provide secure network services:
  - Presence of all SAIFE end points,
  - Coordinate secure sessions on-demand
  - Provide configuration, audit logs, and other command and control
- The TIPRNET cloud resources are designed to be low-value targets:
  - All Black -- All data stored is encrypted and signed, or just signed when not sensitive (such as Remote Wipe commands that must operate even if the device is locked). This capability

provides a highly secure cloud storage mechanism whose access can be cryptographically controlled

- TIPRNET is a collection of federated network components (image on virtual machine, or dedicated hardware)
  - Each is fully redundant, with fail-over should one become unresponsive
  - Undelivered messages persist as they are replicated across the hierarchy (store and forward services)

Presently, TIPRNET Services are located across the United States but is being expanded to Japan, UAE, UK and other areas of operation where high-bandwidth, low-latency secure sessions and connections are desired.

In summary, TIPRNET represents a capability and enables timely, complete dissemination of critical intelligence, leading to decisions and events which directly affect US interests, by utilizing existing open networks and nearly any hardware base across our coalition and interagency partners.

2.3 Use of encryption and key management

Advanced Cryptography Value:

The SAIFE® framework and its capabilities realized through software development kits (SDK) were engineered to the highest security standards for both data-at-rest as well as data-in-transit protection. It is FIPS 140-2 certified and complies with DISA STIG Application Security and Development, MAC II for Classified information. The implementation is compliant with National Security Agency's (NSA) Suite-B cryptographic and data protection standards. The FIPS certification covers a number of processors and operating systems for holistic security across a diverse set of platforms.

Cryptographic agility was designed into the system to leave room for future cryptographic algorithms or for adding backwards compatibility with legacy systems. This was done to provide a graceful growth path using already deployed devices and infrastructure, minimizing impact to users and support structure. It also minimizes impact to the Security Target security architecture and its certification, maximizing both reliability and cost containment of new development.

Certificate-based Authentication & Mobility Value:

Certificate and trust management services provided by SAIFE® provide the foundation for the authentication and encryption of mobile data. SAIFE® realizes a fully implemented public key infrastructure (PKI) which allows for real-time public key distribution and certificate revocation lists. Without exception and for additional security, all certificates are generated within the device and only public key leaves the device. The public key is then used to uniquely identify the device resulting in a network agnostic, authenticated mechanism to address SAIFE®-enabled mobile endpoints. SAIFE®'s trusted public key architecture avoids traditional problems with communicating across diverse user communities. Any set of SAIFE-enabled devices, regardless of their positions within the overall chain of trust, can be permitted to communicate through actions taken only at their respective SAIFE Management server. There is no requirement for the users to share a common trust ancestor, or for a "super" SAIFE® Management server to enable communications. SAIFE® promotes communications agility between any and all of its users, a feature known as AgileTrust™.

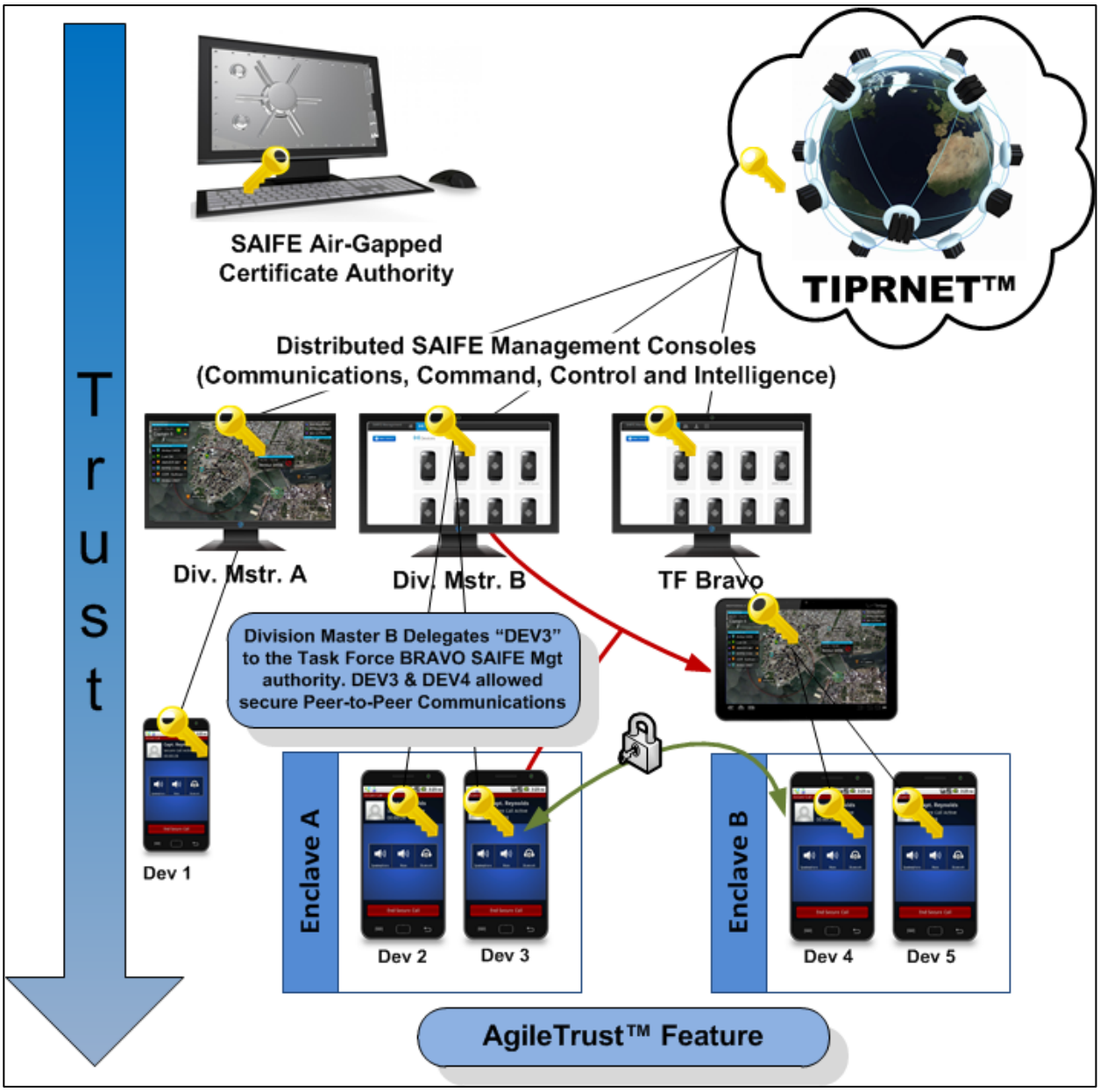

Figure 3 – Overcoming Traditional PKI Deficiencies with SAIFE AgileTrust™

SAIFE®'s unique approach to certificate management enables agile trust relationships to be dynamically established between any SAIFE®-enabled devices. SAIFE®'s PKI infrastructure in conjunction with location information of the end device (e.g. GPS position) allows the formation of geospatial trust domains. Within a geospatial domain, devices can automatically discover other devices located within the same domain (if allowed by the SAIFE Management server), and using public keys, can securely communicate and authenticate the information sent and received. Once a device leaves the geospatial

domain, it no longer can access the devices that are in the geospatial domain. This unique solution, called GeospatialTrust™, allows for the flexible and dynamic establishment of secure enclaves within a well-defined geographical area.

Seamless, Secure Mobility – Removing Infrastructure & Network Boundaries

Another distinguishing feature of SAIFE®'s unique approach to securing mobile endpoints is its implementation of an all-black (Data is never decrypted during transit; It is only decrypted at the endpoint) cloud-based architecture which provides high-availability and low-latency cryptographic services. The architecture realizes bi-directional store-and-forward services for remote configuration, audit logs, key signing, key revocation, software updates, and other management services. Additionally, the scalable infrastructure allows seamless mobility for SAIFE®-enabled devices allowing these devices to reach protected infrastructure components regardless of intervening network topologies. A SAIFE®-enabled device can transition between geographic regions and disjoint networks without sacrificing security or mobility. SAIFE® offers true robust, seamless mobility.

For the transmission of enterprise-related data, SAIFE®'s Cisco-certified VPN offers a standards-compliant IPsec VPN solution for Android-based devices. Combining the power of SAIFE®'s robust and distributed infrastructure with the scalability and feature-rich Cisco ASA, mobile device data can be delivered securely in an encrypted and authenticated tunnel resulting in a low risk solution for protecting sensitive data. Command, control and configuration data for mobile devices traverses SAIFE®'s all-black, cloud-based network while enterprise-related data traverses the SAIFE® Cisco-certified VPN tunnel to Cisco's ASA to fulfil the critical and necessary role of extending protected infrastructure services to the mobile endpoint.

SAIFE® Mobile - Software-Only "SECRET-and-BELOW"[1] on Commercial Android Devices

SAIFE Mobile is a software-only Android (other platforms supported in the near future) application delivering encrypted, authenticated voice and messaging capabilities. Key advantages of SAIFE Mobile over other solutions include:

- Provision and sustain [interoperable] SECRET COMSEC leveraging COTS Android devices (smartphones, tablets, etc.) and commercial cellular/Wi-Fi networks
- SAIFE-enabled – provides logical red/black separation on [unmodified] COTS Smartphones
- End to End COMSEC (data-at-rest, data-in-transit, group management)
- Product features: NSA Suite B protection of SMS/Email/Voice for enclave members
- Real-time Configuration management and OTA provisioning including managed software updates, revocations and remote wipe capabilities

Key SAIFE Mobile Innovations enabling warfighter capability:

1. Built to meet or exceed DoD policy for the protection of data to "Tactical Secret"
   a. When installed on a Type-1 hardware platform, cryptographic libraries can be interchanged to meet Suite A standards

[1] Built to Secret-and-Below standards, presently FIPS 140-2 certified and awaiting NSA certification

2. Comprehensive Data Protection
    a. Data-At-Rest Protections in all application environments
    b. Data-In-Transit Protection
        i. End-To-End cryptographic protection
    c. Authentication Management
        i. Local, Remote wipe
        ii. De-Centralized provisioning and group management
3. Delivers the ability to tie disparate groups together and unify communications schemas
    a. Joint Forces
    b. Coalition Environments
    c. OGA Coordination
4. Delivers a resilient and sustainable platform while containing cost
    a. Over the Air Updates
    b. Remote provisioning allows in-field replenishment
5. Simplified User Experience
    a. Application employs commercial user experience standards and practices
    b. Intuitive Management Interface reduces training time and technical expertise
6. Software-Only
    a. Reduces footprint
    b. Significantly improves portability