

NC4 Homeland Security Cloud™

OVERVIEW

presented by



November 2009

© Copyright 2009 NC4 All rights reserved

CONTENTS

Executive Summary	3
Cloud Computing Background	3
Special Requirements of Cloud Computing in Homeland Security	3
Homeland Security Cloud™ – an NC4 Solution	4
• Solutions for Law Enforcement	4
• Solutions for Emergency Management	5
• Solutions for Secure Communication and Collaboration	5
• Solutions for Situational Awareness	5
NC4 Homeland Security Cloud™ Infrastructure	6
• HSC Infrastructure – Security	6
• HSC Infrastructure – Inter-community and Cross Community Connections	7
• HSC Infrastructure – Situational Awareness	7
• HSC Infrastructure – Information, Document and Process Management	8
• HSC Infrastructure – Information Access	8
• HSC Infrastructure – Mapping and GIS	8
Conclusion	8

Executive Summary

While cloud computing has garnered significant attention in the IT trade press and many corporations have embraced it at least partially, questions of security and privacy of information stored in “clouds” have slowed wide-scale adoption, especially in mission critical applications. This is particularly true in the government sector where much of the data is of a sensitive nature and therefore requires a level of information security not typically available from current cloud-based applications vendors. This white paper describes how the technological and solution foundations for NC4’s Homeland Security Cloud™ meet federal requirements for hosting sensitive data and how they have been operationally proven for years with numerous government agencies.

Cloud Computing Background

Cloud computing refers to the use of Internet (“cloud”) -based technical infrastructure and computing resources to enable convenient, on-demand network access to applications and services. This relatively new and evolving paradigm has grown out of broader trends including the pervasiveness of broad-band Internet access and new low cost technology which allows the virtualization of resources. The benefits of cloud computing are derived from the fact that the entire infrastructure is managed by the cloud provider and the users are able to access a wide variety of applications via an Internet browser. The users of the applications typically have no knowledge or control over the underlying technology in the cloud. Organizations leveraging the cloud computing model can provide these applications at a relatively low cost per user and without the cost and complexity of managing the applications or the IT infrastructure that supports them. For many business applications, this model is ideal because it involves less risk and lower upfront costs as well as flexibility and lower ongoing maintenance costs. The government has recently begun to embrace cloud computing in efforts to modernize IT, reduce costs and speed implementations. Federal CIO, Vivek Kundra believes that cloud computing

is also key to enhancing data sharing and collaboration among federal agencies. The GSA has recently launched the Apps.gov site which provides a directory of available cloud computing applications for office and business productivity and social networking.

Homeland security is an area that has enormous information sharing and analysis needs and can reap huge benefits by implementing cloud computing. The size and complexity of homeland security often result in IT projects that are very expensive and take a long time to implement. Cloud-based solutions offer the promise of lower cost, and faster implementation to help support our nation’s domestic security challenges. However, the nature of homeland security applications and sensitivity of the information being processed present major challenges to the cloud computing model. NC4 has been meeting those challenges for the past several years and has built a unique Homeland Security Cloud™ (HSC) that now serves more than 2,500 organizations in the public and private sector with over 80,000 users. These organizations take advantage of NC4 applications for law enforcement, incident management, situational awareness, and secure communication and collaboration.

Special Requirements of Cloud Computing for Homeland Security

Corporate and government organizations already have valid trepidations in using cloud computing, specifically in the confidentiality and integrity of information stored in cloud-based solutions. These trepidations grow dramatically with homeland security’s need to facilitate the sharing of information at the SBU (Sensitive But Unclassified) and CUI (Controlled Unclassified Information) level. The use of a cloud computing model for these types of applications will require compliance with numerous security standards and the ability to meet federal certifications and accreditations. A key opportunity is that cloud computing for homeland security could support applications which have the potential to deal with organizational silos by providing a level of information sharing and collaboration that spans

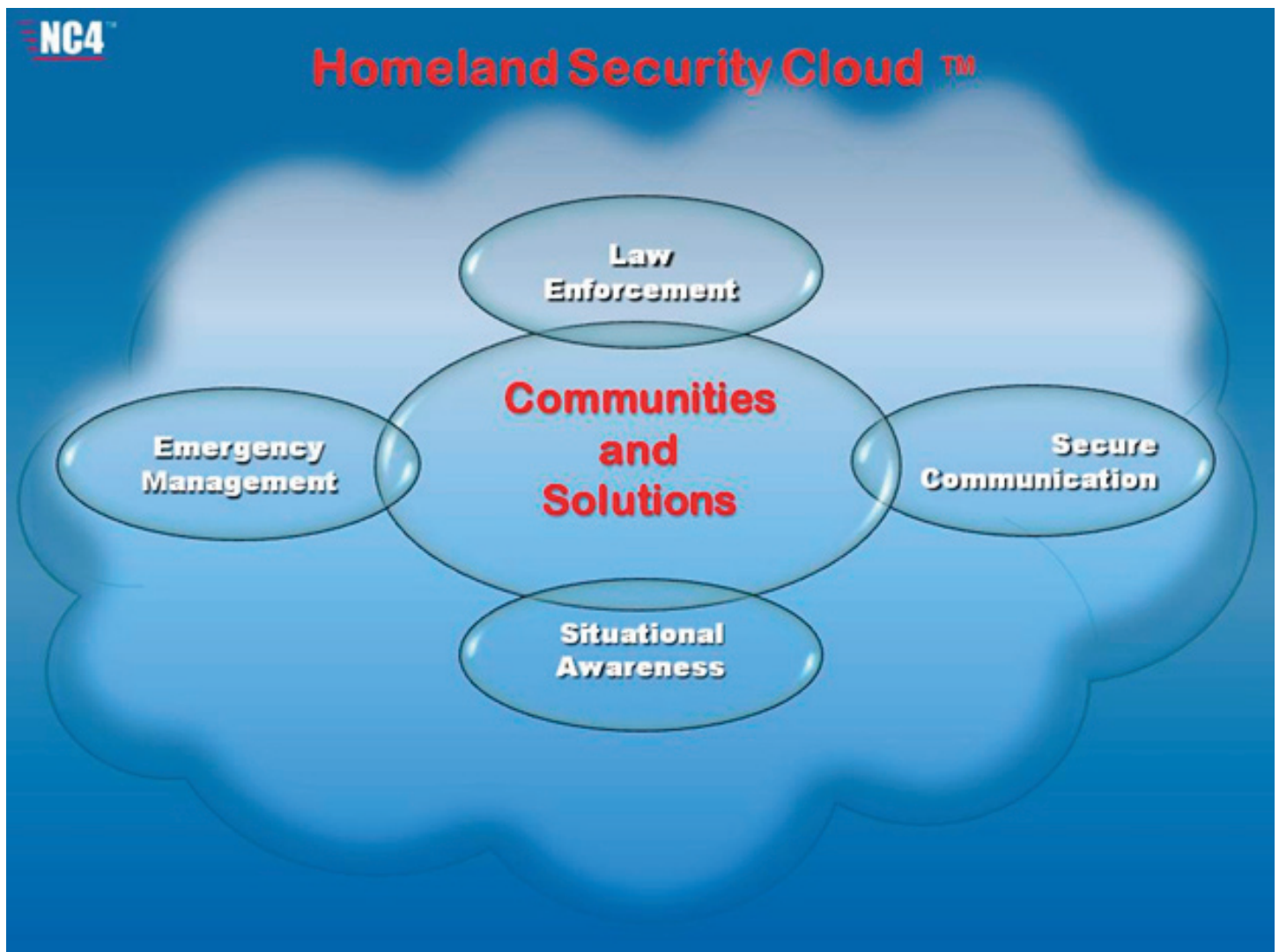
both intra and intergovernmental organizations at the federal, state, and local level and in private sector organizations that support critical infrastructure. In total, supporting confidentiality and integrity of information, reliability of systems and processes, community management, and cross community communications is critical to alleviating security concerns.

Homeland Security Cloud™ - an NC4 Solution

The current NC4 communities and solutions for homeland security cloud computing include Law Enforcement, Emergency Management, Secure Communication and Collaboration and Situational Awareness.

Solutions for Law Enforcement

The NC4 Homeland Security Cloud provides secure information sharing and collaboration services, as well as situational awareness services for over 11,000 law enforcement professionals at the federal, state, and local level. The HSC can provide security for different groups or “compartments”. In total there are over 500 law enforcement compartments which, including our “CyberCop” system allows federal, state, local and international law enforcement professionals to share sensitive information related to other investigations and topics. The NC4 solution is unique in that it meets all pertinent government security criteria, and allows for both open collaboration (common to most cloud applications) and “need-to-know” information collaboration models, essential to disseminating law enforcement information.



Solutions for Emergency Management

NC4 has been a leading supplier of both internal hosted and cloud-based Emergency and Incident Management solutions at the federal, state and local level over the last 5 years. NC4's E Team emergency management solution is also used to support major events such as the Olympic Games, Super Bowls and Homeland Security exercises. Prominent uses of NC4 cloud-based emergency management solutions include the Dallas UASI (Urban Area Security Initiative) implementation.

Solutions for Secure Communication and Collaboration

The NC4 Homeland Security Cloud includes secure communication and collaboration solutions that support a wide variety of missions for numerous federal agencies including the Department of Homeland Security, Department of Energy, NASA, and many others. These solutions provide cloud-based collaboration tools including secure messaging, chat, wiki, discussion forums, document management and mission-focused custom applications. NC4 also maintains a system that provides a secure front end interface that allows users to interact with government clearance databases and satisfy reporting mandates related

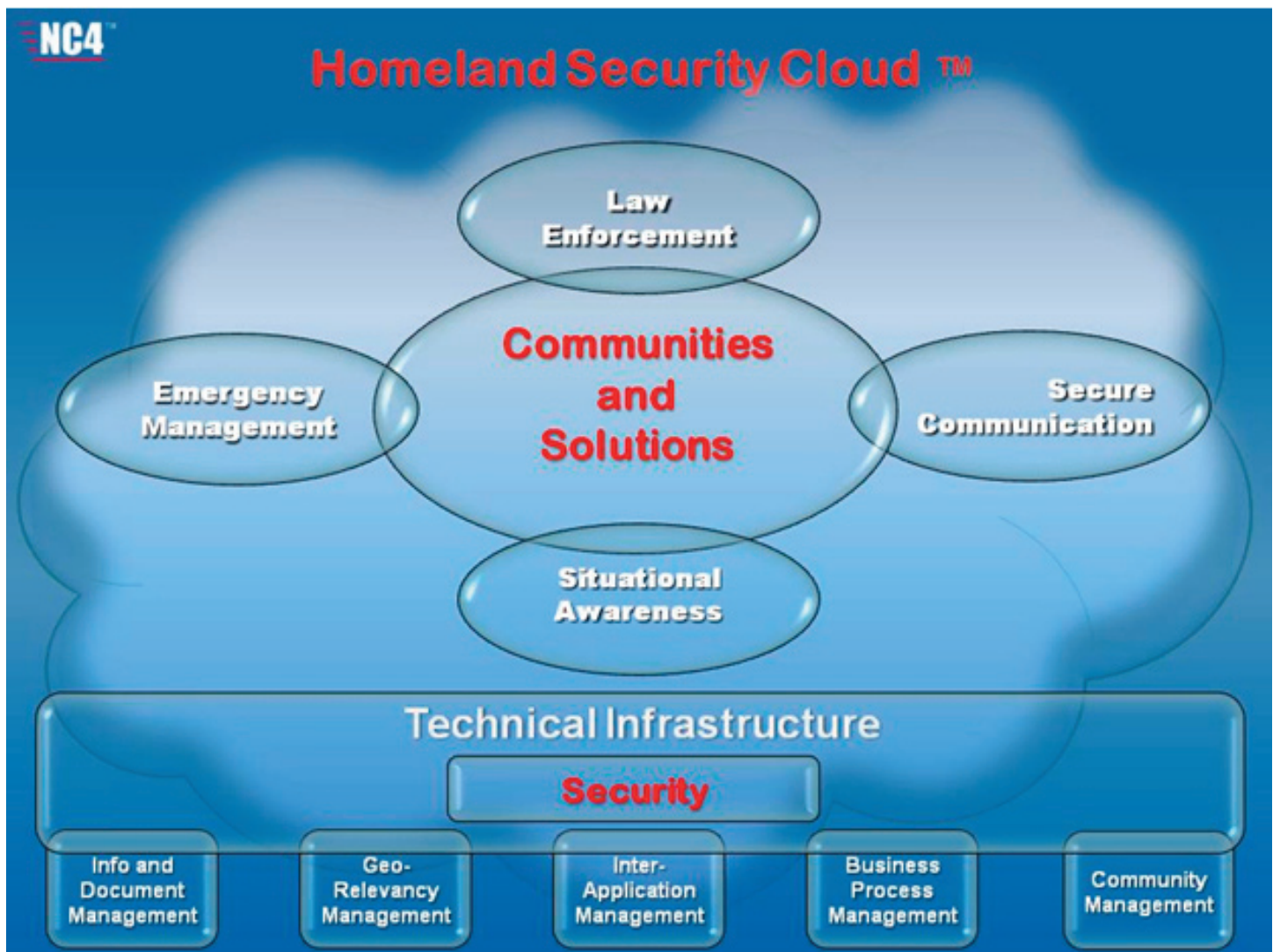
to clearance processing activity. Another mission satisfied by the HSC allows analysts to use collaboration tools and share Control Unclassified (CUI) level information. Participants include representatives from the federal, state, local and tribal levels of government as well as the private sector and international partners. All of these mission applications meet the rigorous security controls required by federal certification and accreditation.

Solutions for Situational Awareness

NC4 provides cloud-based global situational awareness solutions for many federal, state and local government agencies as well as hundreds of large corporations in multiple industries. NC4 operates two 24 x 7 Incident Monitoring centers to collect, filter and summarize incident information from thousands of (primarily local) government and media sources. This information is geo-coded and categorized and sent out as real-time incident alerts based on customer specific profiles. In the first half of 2009, NC4 has monitored over 20,000 unique incidents and delivered over 5 million incident alerts. These alerts are often used by organizations as "trip wires" which initiate further analysis, actions or emergency response using other NC4 cloud-based solutions.



Situational awareness services for the NC4 Homeland Security Cloud™ are provided by two fully redundant incident monitoring centers staffed 24 x 7.



NC4 Homeland Security Cloud Infrastructure

HSC Infrastructure – Security

The NC4 Homeland Security Cloud is a unique offering in the cloud computing space with advanced security features. All applications are hosted in a facility in northern Virginia that was engineered to meet the Director of Central Intelligence Directive Number (DCID) 6/9 guidelines which outline physical security standards for hosting classified data in a sensitive compartmented information facility (SCIF). These protections allow NC4 to meet and oftentimes exceed the protections necessary for hosting sensitive, unclassified information for our customers. In addition to biometric controls on

the perimeter of the facility, NC4 also requires proximity cards, anti-pass-back procedures and federally approved locking mechanisms, such as the X09 lock, for entry into the secure operating center (SOC). Auditable electronic entry logs are maintained for all access control into and out of the facility. The facility was built using continuity of operations specifications to ensure a high level of availability for all NC4 hosted systems. These include an in-line uninterruptible power system with back-up diesel generator, dry pipe fire suppression systems, backup cooling units, humidity controls and active sensors in the event of HVAC failure. The facility also hosts multiple redundant Internet service providers to ensure network availability.

All NC4 operations personnel have been through a preliminary background investigation before being offered an employment position. Individuals that have physical access to our SOC also hold a U.S. Government Secret Clearance sponsored by one of our federal customers.

In addition to the physical and personnel security controls in place at this facility, there are also numerous cyber security controls. NC4's technology has a strong pedigree of cyber security leadership through its beginning at the Defense Advanced Research Projects Agency (DARPA) and its continuation through the Software Engineering Institute of Carnegie Mellon University before the commercialization of its technology. NC4 provides a full cycle security solution enforcing best of breed cyber security practices. These practices also include secure coding and code screening for vulnerabilities throughout the development process including full security scans of all code before it is put into production.

Additional security features of the NC4 Homeland Security Cloud include the following:

- Support for two-factor authentication mechanisms including RSA SecurID and Anakam
- "Need to know" visibility and access models for secure, flexible access control
- Comprehensive user activity audit capabilities for non-repudiation

The security features of the NC4 Homeland Security Cloud have enabled NC4 to achieve multiple certifications and accreditations through compliance with federal security standards including FISMA, NIST 800-53, Title 21 Part 11, 28 CFR part 23 and HIPAA compliance. NC4 has received certifications from multiple federal agencies for the safe hosting of Controlled Unclassified Information (CUI), Sensitive But Unclassified (SBU), For Official Use Only (FOUO), Law Enforcement Sensitive (LES) and medical personally identifiable information. NC4 is audited on an annual basis by federal agency and private sector representatives.

HSC Infrastructure – Inter-community and Cross Community Connections

The NC4 Homeland Security Cloud supports the XML data exchange standards being promulgated by the federal agencies for interoperability between systems. This includes the Common Alerting Protocol (CAP), Emergency Data Exchange Language (EDXL) and National Information Exchange Model (NIEM) standards. Compliance with these standards will allow information sharing between disparate systems more easily and without major changes to the applications.

Another key requirement for information sharing between the NC4 Homeland Security Cloud and other federal government applications is federated identity management. NC4 supports the Global Federated Identity and Privilege Management (GFIPM) framework that provides a standards-based approach for implementing federated identity. This allows users of NC4 Homeland Security Cloud applications to identify and authenticate with other government systems participating in the federation. NC4 is currently part of the GFIPM Security Interoperability Demonstration pilot project sponsored by DHS and the Department of Justice.

HSC Infrastructure – Situational Awareness

NC4 Situational Awareness solutions are supported by proprietary technology to harvest information from thousands of cloud-based information sources. This includes the capability for automated monitoring of Internet-based information sources.

A key part of the HSC infrastructure for Situational Awareness is NC4-developed technology which is used to target relevant incident alerts to the appropriate recipients only. To accomplish this level of relevancy, NC4 developed Geo-Relevancy Management (GRM). GRM refers to the ability to provide automated correlation of incidents with potential impact based on the proximity of the incident to your registered locations. GRM allows a virtual perimeter to be defined around a location

and for a proactive notification to be triggered whenever an incident that meets the profile criteria is reported within the perimeter.

HSC Infrastructure for Situational Awareness leverages the Oracle Real Application Clusters (RAC) technology for load balancing and automated failover between our two geographically separated centers.

HSC Infrastructure – Information, Document and Process Management

NC4 Homeland Security Cloud applications include capabilities in information and document management that are optimized for homeland security missions. This includes an integrated, searchable document repository with workflow approval and expiration date mechanisms and the ability to apply metadata and tags to all content.

The HSC infrastructure also includes the capability for non-technical users to create custom forms using a Web 2.0 drag-and-drop user interface. Rich, dynamic forms can be created with integrated workflow and business rules.

HSC Infrastructure – Information Access

One of the essential tenets of cloud computing is broad network access via a Web browser or mobile device. The HSC Infrastructure is entirely accessible via standard Internet browsers and selected functionality is accessible via Blackberry and other mobile devices.

HSC Infrastructure – Mapping and GIS

Geographical Information Systems (GIS) and mapping are essential components of homeland security solutions. The NC4 Homeland Security Cloud includes integrated support for GIS services including ESRI ArcGIS and ArcIMS and mapping services from both Microsoft and Google.

Conclusion

As corporations and government agencies further explore the intrinsic benefits of cloud computing, they must exercise due diligence in examining their cloud-based applications vendor's ability to provide security and privacy of the cloud infrastructure into which they are entrusting their information. We invite you to contact us to learn more about the NC4 Homeland Security Cloud and how it provides all the advantages of the cloud computing model while also providing the highest level of security for sensitive mission critical applications.