

POSITION PAPER

“Collaborating with Sensitive Information: Serving the Needs of Interoperability and Command and Control”

by Ronald I. Koenig

In “Information Age Transformation: Getting to a 21st Century Military” Dr. David A. Alberts says, “Everyone needs to take a fresh look at what they should consider to be their core competencies. Many will find that some of their traditional competencies are no longer as valuable as they once were and that they need to develop new competencies. In addition, everyone will need to master new competencies that are essential to Information Age organizations. These include sharing of information, quickly and efficiently pulling information from a federation of systems, collaboration, and self-synchronization.”

The President’s 2002 Management Agenda supports “a trusted and interoperable collaboration environment - supported by a full suite of knowledge management (KM) tools and supporting information technology (IT) resources” as defined by the Overseas Presence Interagency Collaboration/KM System wherein inter-agency collaboration is an important goal and a necessity.

According to the U. S. Joint Forces Command, the Collaborative Information Environment (CIE) will not only become an inevitable C2 requirement, but will have the most significant information age impact on Joint Command and Control (JC2). In addition the CIE will:

- Drive the interoperability transformation in Joint C2;
- Prove to be a critical component for both planning and execution;
- Accelerate both C2 processes and organizational changes;
- Require skill, thorough training and proficiency;
- Force the immediate evaluation of available technology today;
- Predetermine the need for interoperable tools and procedures throughout the joint forces for effective C2.

At VIACK Corporation we have been building such a CIE for some time and have done so with the assumption that all CIEs must be highly secure. In addition, this security must be the state of the art and conform to the latest encryption standards for all critical communication requirements. Accordingly, we are pleased to discuss our latest collaborative design, one that is meant to support the ability to provide a multimedia, real time, fully interactive C2 capability to those Government entities where the most sensitive information can never be compromised, anywhere or at any time, and over any type of network. This new capability is called VIA3 for Government.

There is no question that any organization’s most valuable asset is its proprietary and sensitive information. Protecting this information from those who would capture, misuse or abuse it can cost millions of dollars each year. Having this

same information compromised in any way can result in a loss that cannot simply be measured by dollars. Unfortunately, the bulk of today's traditional spending is largely inefficient because it does not go far enough to protect the information itself.

In the private world, organizations spend the majority of their dollars protecting against an unknown, outside threat—typically in the form of a hacker or someone with malicious intent. What most fail to realize is that their threats are far more likely to come from where they least expect it—from within their own “trusted” groups.

In 80% of reported security breaches found in a 2003 survey conducted by the Computer Security Institute and FBI, the cause of the breach was due to insider abuse of network access. That means a disgruntled member of your own organization, with the know-how and intent can take your most precious information and use it against you. Fortunately, there is now a solution.

VIA3 for Government: The Ultimate Information Gatekeeper

VIA3 for Government is the only managed service that enables the military, agencies and companies to pre-selectively determine classification of—and access to—all assets. VIA3 for Government creates a hierarchy for personnel, documents, and facilities, and in addition, automates the high level functions of a chief security officer. Access to all assets is granted based on an individual's need—and right—to know information.

By denying persons without proper clearance the ability to access sensitive information, organizations can eliminate the likelihood of costly security breaches. We are not simply identifying another information rights management tool, but a uniquely comprehensive capability that will provide anyone with the proper need and right to know, the ability to conduct highly sensitive operations over any network, whether private or public anywhere and at any time. Imagine the possibilities.

Highest Levels of Encryption Allowed by Law

VIA3 for Government includes comprehensive security that is unprecedented in the industry. All parts of the product are protected with AES, which is not only the new government standard for encryption, but is also the highest level of encryption available for significant security challenges, command and control, intelligence and any other situation where there can never be any compromise.

There are four levels of security included in VIA3 for Government:

- **Contacts** - Each contact that you communicate with is granted a level of security based upon his/her assigned access level
- **Files** - Each file stored in an electronic file cabinet contains a security classification indicating its level of confidentiality
- **File Cabinets** - Files are held within electronic file cabinets with access granted only to those that meet the highest level of clearance required by the documents contained within it
- **Subject Matter Index** - Regardless of someone's level of clearance, their ability to access a particular file is based on their need and right to know such information

The Power to Protect Classified Information

By utilizing VIA3 for Government in the CIE, your command will:

- Eliminate the purposeful or inadvertent release of classified documents
- Create specific rules for documents and personnel according to their classification, such as prohibiting downloading or printing sensitive information
- Sign in and out documents, allowing you to track who has accessed the information
- Collaborate securely with others in real time
- Log any suspicious attempts at accessing confidential information, and immediately alert a security office
- Support full authentication for Smart Cards and biometrics

CIE with a Full Feature Set

In VIA3 for Government, VIACK uses the same high levels of privacy offered in the company's flagship product, VIA3 E-meeting Service. Once the proper authorization on a document has been established between individuals with VIA3 for Government, they can use the other collaborative features within the e-meeting service. These features include:

- **Live Audio and Video:** See and hear others in your e-meeting
- **Instant Messaging:** Quickly send secure private messages to others
- **Presentation Sharing:** Share and annotate Microsoft PowerPoint® presentations in real time
- **Joint Edit:** Enter, merge, and track revisions in one central Word® or Excel® document

- **File Cabinets:** Create permission-based, online workspaces where sensitive files can be securely shared and stored
- **Screen Capture:** Bring spreadsheets, images, Web pages, or anything you can see on your computer into an e-meeting
- **Whiteboard:** Visually express ideas and comments with the ability to brainstorm, draw, mark-up, and save graphical information

This newest service will provide a finely discrete, user-defined set of locks, gates, filters and rules to provide an agency, military command or company with the absolute control over who with the proper vetting can access what information, and where and how that information is accessed. Most collaborative services have only cursory security and/or secure only a portion of the collaborative suite of functions. VIACK strongly believes, as is evident in the services we provide, that no one can be almost secure. It must be absolute.

About the Speaker

Ronald I. Koenig serves as Chairman, President and CEO of VIACK Corporation.

With more than 42 years of software design, development, and senior management expertise, Ronald is a true computer industry pioneer.

Beginning his work in 1959, after obtaining an engineering and work study scholarship award with the United States Navy, he then joined the United States Air Force in 1962 specifically to study computers and operating systems. In 1967, Ronald was chosen to retrain the most capable senior members of both the Air Force and civilian community regarding a new, highly innovative computer and software acquisition awarded to Burroughs Corporation. These systems utilized design concepts which would still be considered quite innovative today.

Starting in 1970 and for many years thereafter, Ronald designed and built both large and medium-scale mainframe operating systems and was involved in numerous hardware and software engineering projects for Burroughs Corporation prior to their merger which created Unisys. Within Burroughs, Ronald was also a turnaround expert in resurrecting failing major commercial accounts like Pacific Telephone resulting in significant new revenue.

In various senior management capacities, Ronald has led large manufacturing, data processing, and telecommunications organizations, and he has solely owned, operated, expanded, and successfully sold several manufacturing and engineering companies. Ronald earned a BS degree in Business Administration from Columbia College and an MBA from Alameda College.

###