# KUSA White Paper:

# Cyber-Secure Video & Clean Code Technology For Securing SCADA and Contol Networks

Technical Support, Engineering, Planning, Training, & Risk Assessment

## Is Your Network

## Being Watched

## or

## Watched Over?

KUSA - An American ECO Engineering Company

# White Paper: A SCADA Strategy to Secure Cyberspace with CYBER-SECURE Video / Data

## CYBER-SECURE VIDEO / DATA with Clean Code Technology

The document is partially based on the US National Strategy to Secure Cyberspace (www.us-cert.org) with the permission of US-CERT. This document also describes CYBER-SECURE Video / Data, Clean Code Technology and its attendant mechanisms within Secure Cyberspace. Certain elements of this technology are not for public dissemination and therefore are not discussed in any detail. This work is part of the research accomplished by the Software Engineering Institute (SEI) for Cyber Security.

# Summary

SCADA systems critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, as well as postal and shipping. Cyberspace is the nervous system—the control system of a building, city, county, municipality, state or country.

The SCADA Cyberspace is composed of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow the critical infrastructures to work. The healthy functioning of cyberspace is essential to the economy, safety and our national security.

The purpose of this document is to engage and empower network operators to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the central and local governments, the private sector, and individual people, such as yourself.

A large proportion of the systems we rely upon as a society are poorly protected, and barely managed. These systems run 24 hours a day without incident. It is now apparent that leaving these systems unguarded and un-protected will increase our risk profile, now and in the future. New technologies to secure network equipment as well as video and data streams are required to achieve secure communication. The ability of an Ethernet device to resist virus and BOT infection is now a priority for mission critical services. This capability requires precision coding techniques along with clean code. Silicon enhancements, precision coding techniques and the use of “Clean Code Technology” allows network operators to begin the process of fully securing their networks.

Network security is a layered process. It involves many steps, such as limiting network access and connectivity, securing wireless connections, as well as physical security. We will discuss several aspects to this layered approach in this paper.

Currently – the conventional wisdom in network security calls for a perimeter defense. A walled fortress approach with the hostile elements being kept outside is the methodology currently being deployed. This model is based on 20th Century network architecture. Hard shell on the outside – with soft unprotected network targets on the inside.

Our 21st Century architecture calls for the hardening and protection of the inside network elements to prevent code and virus contamination, including BOT prevention and Denial of Service attacks. This strategy requires clean uncontaminated code that works to prevent unintended intrusion and corruption of data. These are the basic elements of Cyber-Secure Video, with Clean Code Technology.

The *National Strategy for Secure Cyberspace* outlines an initial framework for both organizing and prioritizing cyber security efforts. It identifies steps that the government, private companies and organizations, manufacturers and individuals can take to improve their collective cyber security. The *Strategy* highlights the role of public-private engagement. The document provides a framework for the contributions that are to be made to secure their part of cyberspace and the critical infrastructure it connects. The dynamics of cyberspace will require adjustments and amendments to the *Strategy* over time.

The speed and anonymity of cyber-attacks makes it difficult to distinguish the attackers. The task often occurs only after the fact, if at all. Therefore, the *National Strategy for Secure Cyberspace* helps reduce our country's vulnerability to destructive attacks against our critical information infrastructures or the physical assets that support them.

CYBER-SECURE Video / Data (CSV) is a methodology implemented at the root of computing machine to machinery (M2M) technology aligned with the coding techniques as recommended by the *National Security Agency (NSA) / Central Security Service (CSS)- Cryptologic Division.* Embedded code is used to secure machine functionality and the secure routing of packets from and to the intended source /target. Precision coding techniques further enhance the device's ability to resist outside BOT and Virus infection. A combined "Clean Code" technique is used to insure the absence of malware, bots, viruses and other security threats, often found in commercially available hardware and software. Today – you can find many lines of corrupted old software contained within software stacks – that were once functional, but now have no use. This unused code may be used by attackers as a backdoor for malicious intentions. The use of clean code technology is used to prevent the corruption of the network devices themselves and insure the intended operation of the network equipment. These elements and other security practices are vital in producing secure SCADA and Control networks. Education, knowledge and planned procedures will all help to secure our infrastructure and produce better networks. This original research has been accomplished by the Software Engineering Institute (SEI).

## Strategic Objectives

The strategic objectives of the *National Strategy for Secure Cyberspace* are to:

- Prevent cyber-attacks against critical infrastructures;
- Reduce national vulnerability to cyber-attacks; and
- Minimize damage and recovery time from cyber-attacks that do occur.

The strategic objectives *of CYBER-SECURE Video/Data* are to:

- Secure data & video streams from being mirrored or duplicated without the knowledge of the network operator.
- Maintain clean machine code without the introduction of outside and unintended coding elements.
- Minimize hacking, virus and BOT introduction to SCADA network equipment.
- The elimination of unintended coding elements present in commercial non-secure products.
- Protection, verification and authentication of frame data within networks.

## Threat and Vulnerability

Our economy, safety and national security are dependent upon information technology and the information infrastructure. At the core of the information infrastructure upon which we depend is the Internet, a system originally designed to share unclassified research among scientists who were assumed to be uninterested in abusing the network. It is that same Internet that today connects millions of other computer networks making most of the nation's essential services and infrastructures work. These computer networks also control physical objects such as electrical transformers, trains, pipelines, pumps, chemical vats, radars, traffic lights and stock markets, all of which exist beyond cyberspace.

A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber-attacks capable of causing disruption to our critical infrastructures, economy, or national security.

The required technical sophistication to carry out such an attack is high—and partially explains the lack of a destructive attack to date. However, there have been instances where organized attackers have exploited vulnerabilities that may be indicative of more destructive capabilities. One such recent attack occurred on a kidney dialysis (2011) machine here in the United States. The attack was not malicious, but instructive as to the vulnerability of our infrastructure. On a national scale, the NSA in conjunction with our power utility companies demonstrated the capability of destroying power generating equipment remotely. On a world scale – Iran had its Siemens uranium centrifuges destroyed by the STUXNET worm. This virus was able to single out Siemens controllers, and destroy or render them useless .

Uncertainties exist as to the intent and full technical capabilities of several observed attacks. Enhanced cyber threat analysis is needed to address long-term trends related to threats and vulnerabilities. What is known is that the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving. Our enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the country's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems. Something as simple as shutting down a waste treatment plant – could have devastating consequence for the targeted community.

Cyber-attacks on information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructures. These attacks are indicative of the need for "Cyber-Secure Video / Data (CSV)" and "Clean Code Technology.

## Critical Priorities for Cyberspace Security

The *National Strategy for Secure Cyberspace* articulates five general priorities including:

1.) A National Cyberspace Security Response System (Computer Emergency Response Team, CERT).
2.) A National Cyberspace Security Threat and Vulnerability Reduction Program..
3.) A National Cyberspace Security Awareness and Training Program.
4.) Securing Governmental Cyberspace
5.) National Security and International Cyberspace Security Cooperation.

The first priority focuses on improving our response to cyber incidents and reducing the potential damage from such events. The second, third, and fourth priorities aim to reduce threats from, and our vulnerabilities to, cyber-attacks.

The fifth priority is to prevent cyber-attacks that could impact national security assets and to improve the international management of and response to such attacks.

### 1) A National Cyberspace Security Response System

Rapid identification, information exchange, and remediation can often lessen the damage caused by malicious cyberspace activity. For those activities to be effective at a national level, we need a partnership between Internet NGOs, industry and government, to perform analyses, issue warnings, set up standards and coordinate response efforts.

Privacy and civil liberties must be protected in the process. Because no cyber security plan can be unreceptive to sophisticated and intelligent attack, information systems must be able to operate while under attack and have the resilience to restore full operations quickly.

The *National Strategy for Secure Cyberspace* identifies eight major actions and initiatives for cyberspace security response:

1. Establish public-private architectures for responding to national-level cyber incidents.
2. Provide for the development of tactical and strategic analysis of cyber-attacks and vulnerability assessments.
3. Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace.
4. Expand the Cyber Warning and Information Network to coordinate crisis management for cyberspace security.
5. Improve incident management and reporting.
6. Coordinate processes for voluntary participation in the development of national public-private continuity and contingency plans.
7. Exercise cyber security continuity plans for government systems.
8. Improve and enhance public-private information sharing involving cyber-attacks, threats, and vulnerabilities.

### 2) A National Cyberspace Security Threat and Vulnerability Reduction Program

By exploiting vulnerabilities in our cyber systems, an organized attack may endanger the security of our critical infrastructure and support systems..

The vulnerabilities that most threaten cyberspace occur in the information assets of critical infrastructure enterprises themselves and their external supporting structures, such as the mechanisms of the Internet. Lesser-secured sites on the interconnected network of networks also present potentially significant exposures to cyber-attacks. Vulnerabilities result from weaknesses in technology and because of improper implementation and oversight of technological products, processes and coding techniques.

The *National Strategy for Secure Cyberspace* identifies eight major actions and initiatives to reduce threats and related vulnerabilities:

1. Enhance law enforcement’s capabilities for preventing and prosecuting cyberspace attacks.
2. Create a process for vulnerability assessments to better understand the potential consequences of threats and vulnerabilities.
3. Secure the mechanisms of the Internet by securing and improving protocols and routing.
4. Foster the use of **trusted digital control systems/supervisory control and data acquisition systems.**
5. Reduce and remediate software vulnerabilities and produce clean code network security products.
6. Understand infrastructure interdependencies and improve the physical security of cyber systems and telecommunications.
7. Prioritize cyber security research and development agendas, including Cyber-Secure Video / Data, Clean Code Technology, network and packet signature analysis, and silicon blocking.
8. Assess and secure emerging SCADA and Control systems.

### 3) A National Cyberspace Security Awareness and Training Program

Many cyber vulnerabilities exist because of a lack of cyber security awareness on the part of computer users, systems administrators, technology developers, procurement officials, auditors, chief information officers (CIO), chief executive officers (CEO), and corporate boards.

Such awareness-based vulnerabilities present serious risks to critical infrastructures regardless of whether they exist within the infrastructure itself. A lack of trained personnel and the absence of widely accepted, multi-level certification programs for cyber security professionals complicate the task of addressing cyber vulnerabilities.

The National Strategy for Secure Cyberspace identifies four major actions and initiatives for awareness, education, and training:

1. Promote a comprehensive national awareness program to empower all businesses, the general workforce, and the general population—to secure their own parts of cyberspace.
2. Foster adequate training and education programs to support the Nation's cyber security needs.
3. Increase the efficiency of existing government cyber security training programs.
4. Promote private-sector support for well-coordinated, widely recognized professional cyber security certifications, products and code types.

### 4) Securing Governmental Cyberspace

Although governments administer only a minority of our critical infrastructure computer systems, governments at all levels perform essential services in the agriculture, food, water, public health, safety, emergency services, defense, social welfare, information, telecommunications, energy, transportation, banking, finance, chemicals, postal and shipping sectors that depend upon secure and unadulterated cyberspace for their service delivery. Governments can lead by example in cyberspace security, including fostering a marketplace for more secure technologies through their procurement.

The National Strategy for Secure Cyberspace identifies five major actions and initiatives for the securing of governments' cyberspace:

1. Continuously assess threats and vulnerabilities to government cyber systems.
2. Authenticate and maintain authorized users of government cyber systems.
3. Secure government wireless local area networks, and the acquisition of secure network elements.
4. Improve security in government outsourcing and procurement, and the use of clean code technology.
5. Encourage central and local governments to consider establishing information technology security programs and participate in information sharing and analysis centers with similar entities.

### 5) National Security and International Cyberspace Security Cooperation

Our cyberspace links us to the rest of the world. A network of networks spans the planet, allowing malicious actors on one continent to act on systems thousands of miles away. Cyber-attacks cross borders at light speed, and discerning the source of malicious activity is difficult. We must be capable of safeguarding and defending its critical systems and networks. Enabling our ability to do so requires a system of cooperation to facilitate information sharing, reduce vulnerabilities, and deter malicious actors.

The National Strategy for Secure Cyberspace identifies five major actions and initiatives to strengthen our national security and internal cooperation mechanisms:

1.) Strengthen cyber-related counterintelligence efforts.
2.) Improve capabilities for attack attribution, signatures and response.
3.) Improve coordination for reporting and responding to cyber-attacks within the security community.
4.) Work with industry and through organizations to facilitate dialogue and partnerships among public and private sectors focused on protecting information infrastructures and promoting a global "**culture of security;"**
5.) Foster the establishment of regional and national watch-and-warning networks to detect and prevent cyber-attacks as they emerge.

# A Strategic National Effort

Protecting the widely distributed assets of cyberspace requires the efforts of many organizations. The government alone cannot sufficiently defend cyberspace. It is required that organizations outside the government take the lead in many of these efforts. Everyone who can contribute to securing part of cyberspace should be encouraged to do so. The intelligence community invites the creation of, and participation in, public-private partnerships to raise cyber security awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information, and plan recovery operations.

## Cyberspace Infrastructure

Our critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information, telecommunications, energy, transportation, banking, finance, chemicals, and hazardous materials, postal and shipping. Cyberspace is the nervous system of these infrastructures—the control system of the country. Cyberspace comprises thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security. However, we are aware of the existence of cyberspace vulnerabilities and the fact that malicious actors seek to exploit them.

This National Strategy for Secure Cyberspace is part of an overall effort to protect the connected assets and services. The purpose of this document is to engage and empower network operators, to secure the portions of cyberspace that they own, operate, or control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the central and local governments, the private sector, and people like you.

## A Unique Problem, a Unique Process

Most critical infrastructures, and the cyberspace on which they rely, are privately owned and operated. The technologies that create and support cyberspace evolve rapidly from private sector and academic innovation. Government, and security mandates alone cannot sufficiently secure cyberspace.

Thus, there is a call for voluntary partnerships among government, industry, academia, and nongovernmental groups to secure and defend cyberspace.

In recognition of this need for partnership, the process to develop a Strategy for Secure Cyberspace included soliciting views from both the public and private sectors. The Strategy is not immutable; actions will evolve as technologies advance, as threats and vulnerabilities change, and as our understanding of the cyber security issues improves and clarifies. The dialogue on cyberspace security must therefore continue.

# National Cyberspace Security Priorities

*The National Strategy for Secure Cyberspace* is a call for national awareness and action by individuals and institutions, to increase the level of cyber security worldwide and to implement continuous processes for identifying and remedying cyber vulnerabilities. Its framework is an agenda of five broad priorities that require widespread voluntary participation. Addressing these priorities requires the volunteer leadership of some organizations. They must take the task of translating the Strategy's recommendations into actions.

Corporations, universities, and local governments, and other partners are also encouraged to take actions consistent with these five national cyberspace security priorities. Each private-sector organization must make its own decisions based on cost effectiveness analysis and risk-management and mitigation strategies.

## Securing SCADA Cyberspace

Although SCADA operators administer only a minority of the critical infrastructure computer systems, service organizations at all levels perform essential services that rely on each of the critical infrastructure sectors, which are agriculture, food, water, public health, emergency services, government, defense industrial base, information, telecommunications, energy, transportation, banking, finance, chemicals and hazardous materials, postal and shipping. With respect to investment in cyberspace security, government can lead by example by fostering a marketplace for more secure technologies through large procurements of **advanced information assurance technologies**.
A program to implement such products will help to ensure that governmental computer systems and SCADA networks are secure.
Steps to take:
(1) Make IT security a priority in higher education.
(2) Revise institutional security policy and improve the use of existing security tools.
(3) Improve security for future research and education networks.
(4) Improve collaboration between higher education, industry, and government,
(5) Integrate work in higher education with the national effort to strengthen critical infrastructure.
.
Training
In addition to raising general awareness, network operators must focus resources on training a talented and innovative pool of personnel that can specialize in securing the infrastructure. While the need for this pool has grown quickly with the expansion of the Internet and the pervasiveness of computers, networks, and other cyber devices, the investment in training has not kept pace. Universities are turning out fewer engineering graduates, and much of their resources are dedicated to other subjects, such as biology and life sciences.

### KUSA Position Statement

## Reduce Vulnerabilities in the Absence of Known Threats

**(Common Security Vulnerabilities in today's SCADA networks)**:

**Un-managed Ethernet Networks** – Many Ethernet networks today are built upon non-managed Ethernet products. The attractiveness of these products is that there is no addressing to be configured. They are referred to as "PLUG N PLAY" devices. These networks are the most vulnerable SCADA and Control networks. These devices have no control of the ports, or the devices that are plugged into them. **There is a total absence of any type of security.**

Un-managed Ethernet products will not meet the new federal guidelines for the security and lockdown measures required for SCADA and control networks. These networks are extreme security risks, non-scalable, and difficult to troubleshoot. When a cyber-security breach occurs – time and control of a network is essential. The new federal guidelines mandate the security and lockdown of both used and unused ports. That means – you must be capable of turning off unused ports and locking the known MAC address and/or IP address of the attached device.

These un-managed Ethernet devices, due to their sparse silicon elements, are subject to BOT attacks and viruses. They have very poor code control, and are known security risks.

**Managed Ethernet Networks** – A new generation of Managed Ethernet devices have the capability of meeting the new federal guidelines for securing SCADA and control networks. Every port can be turned on and off. Port statistics are available from each port and trunk. New federal guidelines require that unused ports be turned off or rendered useless.

These new managed devices implement SNMPv3 and SSH for communications. Both SNMPv3 and SSH provide encrypted packet texts and do not broadcast machine or device information in clear text across the network. (Telnet and its clear text must be eliminated)

Implementation of Sticky MAC / Port Lock down – means that the network operator freezes or locks down the MAC addresses learned on each port. Every Ethernet switch in operation today "learns" the MAC addresses of all attached devices and those that "pass thru". If an existing device is unplugged and a new device is plugged in – the new MAC address will trigger and automatic port shutdown and generate an SNMP alarm.

Implementation of IP Address / Port Lock down – means that the network operator freezes or locks down the IP addresses learned on each port. Again, all present day switches and routes "learn" the IP addresses of all devices attached or "pass thru". If an existing device is unplugged and a new device is plugged in – the new IP address will trigger an automatic port shutdown and generate an SNMP alarm.

The dual lockdown of IP & MAC addresses makes spoofing a device much more difficult for a cyber-attacker.

It is also recommended in the new federal security guidelines that networks be segmented into smaller collision & broadcast domains via addressing and layer 3 connectivity. There is no reason to have the receptionist directly attached to your SCADA or control system. SCADA and control systems should be subject to greater command and control and need to have limited, recorded and verifiable access. If you can ping critical infrastructure from the receptionists pc – you have a problem that MUST be remedied. This is not to say that you can expect an attack on the infrastructure from your receptionist. It is indicative of a poorly structured network design.

Another common network mistake is to leave product passwords unchanged from the factory. This has been done by both large and small organizations.

Until now our security measures have mostly fallen into perimeter defense. This type of defense has been our primary architecture during the last century. Build a network – and plug a firewall into it. While this is important, the security and adulteration of network devices themselves have largely been ignored. What happens inside your network once intruders get in? Contaminated and weak code from around the world is often used in cut rate network products – putting your network and services at risk. What we mean here is that so much more memory is available to today's programmers that the elimination of extraneous code is all but non-existent. There no longer is a requirement to "clean up" written code stacks, often leaving behind code that can be used by perpetrators to invade a given network for destructive or snooping purposes.

While it is still important to secure the perimeter of your network – it is also important to secure network elements and the code that runs upon them. This is the new methodology for securing your 21st Century network. Using scientifically engineered code can thwart cyber-attacks before they start. Simple things like auto detection of Denial of Service (DDOS) attacks are important measures to take in the security of a network.

**KUSA is committed to the engineering, manufacturing and installation of network elements that adhere to the mandates being made by *The National Strategy for Secure Cyberspace.* Our new products have a variety of cyber security features engineered into each product. Clean code is in all of our products.**

## New Clean Code Technology Examples:

**DOS / DDOS Attacks:** Our new managed series Power over Ethernet switches have the capability to **automatically** prevent "Denial of Service (DDOS) attacks. A Denial-of-Service attack (DoS attack) or Distributed Denial-of-Service Attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers.

KUSA's switches are engineered with an advanced **DoS/DDoS auto-prevention** feature. If there is a rapid increase of traffic flow in a short time, (dependent upon frame size and signature). The KUSA Cyber-Secure switch will lock the source IP address for certain time to avoid the network from being attacked. Since this is a hardware-based prevention mechanism, it can prevent large scale DDoS attack immediately and completely, without the network operator's intervention.

**Device Binding:** KUSA's managed switches with Cyber-Secure Video - effectively *binds* the IP/MAC address of the device connected with the switch port. If the IP/MAC address of the connecting device does not match the switch port binding information, the device will be blocked for security. Additionally, the bound device also benefits from a collection of active network traffic protection and maintenance tools — alive check, stream check, and DoS/DDoS auto-prevention. **Device Binding** actively blocks hacker attacks and ensures that all network bound devices are running well. Every port is secure and monitored, all the time and with no interruptions.

The examples listed above, are but a small slice of the capabilities built into our new technology devices. "KUSA – **Network Security For The 21st Century**

*Acknowledgements:*

*We offer our sincere appreciation to the following contributors to this general information white paper and to the many researchers who shared their knowledge.*

*US National Strategy to Secure Cyberspace (US-Cert,org)*
*NSA / CSS Cryptology Division – Cyber Research*
*European Union Cyber Security Committees*
*Software Engineering Institute (SEI) – Carnegie Mellon University*
*JOSH Transportation Systems*

*John Effington – Cyber-terrorism Consultant*
*Center for Threats and Assessment*
*Blue Dragon Consulting – Network Security (www.bluedragon-consulting.com)*
*KUSA – Security Engineering*

KUSA
1107 SE Willow Place
Blue Springs, Missouri, 64014

Telephone: (219) 595 - 2632
(219) KYLAND 1
FAX: (480) 287 - 8605
Email: Sales@Kyland-USA.com