Industry Observations on the Emerging Cyber Security Market

Prepared for:

Virginia Cyber Security Commission
Town Hall

By:
George Hughes, SimVentions President

Overview of Briefing

- Cyber Security milestones & observations
- SimVentions overview and involvement in Cyber Security market
- Stafford Technology & Research Center
- What can Virginia do to help Cyber Security businesses develop solutions for our rapidly growing national threat(s)?

Cyber Warfare Milestones

1969	**December** ARPA (Advanced Research Projects Agency) goes online and connects four major U.S. universities. Designed for research, education, and government organizations, it provides a communications network linking the country in the event that a military attack destroys conventional communications systems.
1982	**June** After learning that the **Soviet Union planned to steal software from a Canadian company** to control its Trans-Siberian Pipeline, the CIA alters the software to cause the pipeline to explode. It is considered the first cyberattack.
1986	Over the course of 10 months beginning in August, Clifford Stoll, a physics researcher at the University of California at Berkeley, tracks down a **hacker who had broken into computers at the Lawrence Berkeley National Laboratory**, a U.S. Department of Energy facility, and other military computers in the U.S. He **traced the hacker to Germany**. It is the first such investigation.
1988	**November** An **Internet worm temporarily shuts down about 10% of the world's Internet servers**. It is the first occurrence of an Internet worm. Robert Tappan Morris, a **student at Cornell University, released the worm**. Morris is the first person tried and convicted under the computer fraud and abuse act.
1994	**March and April** Computers at the Rome Air Development Center at Griffiss Air Force Base in New York are attacked 150 times by anonymous hackers, who use a "**sniffer" program to steal login credentials and sensitive information from the lab**, which conducts research on artificial intelligence systems, radar guidance systems, and target detection and tracking systems. The **hackers then use the login information to access the computers of other military and government facilities, including NASA's Goddard Space Flight Center and the Wright-Patterson Air Force Base**.

Cyber Warfare Milestones

1997	**June** The NSA conducts a test, known as Eligible Receiver, to assess the vulnerability of government and military computers to a cyberattack. The **exercise reveals that systems throughout the country could be hacked and disrupted with relative ease using commercial computers and software**.
1998	**February** Analysts with the Air Force Computer Emergency Response Team in San Antonio, Texas, notice intrusions into their computer networks from several academic institutions, including Harvard. The **hackers, who turned out to be three teenagers**, exploited a weakness in the network's operating system. The event is a wake-up call to the government and prompted President Bill Clinton to develop a cyber-security plan. **December** The Department of Defense establishes the Joint Task Force on Computer Network Defense to defend the department's networks and systems "from intruders and other attacks."
2001	**July** The **worm named Code Red** affects computer networks running a Microsoft operating system. Some websites, including the **White House site, are disabled**.
2003	Anonymous, the group of hackers who refer to themselves as "Internet activists" and attack government, corporate, and religious websites, is organized. While the group avoids adhering to a strict philosophy, its members seem united in their opposition to censorship. **February** President George Bush announces the creation of a new office under the Department of Homeland Security, the National CyberSecurity Division, and lays out a National Strategy to Secure Cyberspace to protect the nation's computer and information systems from a cyberattack. **November** **Hackers, believed by U.S. officials to be backed by the Chinese military**, search to find vulnerable computers in the military's computer network and steal sensitive information. The attacks continued for about **three years and were given the name Titan Rain** by U.S. officials.

Cyber Warfare Milestones

2006	**December** NASA begins to block emails with attachments prior to the launch of space shuttles to prevent hackers from sabotaging launch plans by gaining unauthorized access to the agency's computer network.
2007	**April–May** **Estonia's government websites are hacked** by distributed-denial-of-service-attacks and are compromised for 22 days. The **hackers are believed to be backed by the Russian government**. Targets include the **president's office, Parliament, law enforcement officials, and Estonia's two biggest banks**. **June** The **email account of U.S. Secretary of Defense** Robert Gates is hacked. **Officials blame China's** People's Liberation Army. **September** **British government officials announce that hackers** have breached the computers of the Foreign Office and other government agencies. The **hackers are believed to be members of China's** People's Liberation Army.
2008	**July** **In the weeks before the war between Russia and Georgia, Georgia is hi**t by distributed-denial-of-service-attacks and many of the government's computer networks are disabled, including that of President Mikheil Saakashvili. Media and transportation companies are also affected. **Georgian officials accused Russia** of launching the attack. **October** **Pentagon officials discover that a flash drive containing a covert program** was inserted into a laptop at a base in the Middle East. The **program collected data from a classified Department of Defense computer network and transferred it to computers overseas**. Government officials say the hack was carried out by a foreign intelligence agency and called the intrusion, "most significant breach of US military computers ever."

Cyber Warfare Milestones

2009	**January** **Israel's government Internet sites are attacked during the conflict with Hamas** in the Gaza Strip. Government computers are barraged with as many as 15 million junk emails per second, and the computers are temporarily paralyzed. Israel suspects Hamas financed the hack. **March** Canadian researchers at the Munk Center for International Studies at the University of Toronto, announce that **hackers based in China had penetrated almost 1,300 computers in 103 countries**, including those belonging to embassies, government offices, and the Dalai Lama, and stole documents and other information. **December** News reports say that **Iraqi insurgents had hacked into live feeds being sent by U.S. drones** to military officials on the ground.

Cyber Warfare Milestones

April

University of Toronto researchers report that **hackers broke into India's Defense Ministry** and stole classified information about the country's national security system. The **report, which points the finger at China**, also says that the computers of embassies throughout the world had been compromised.

June

Security experts discover Stuxnet, the world's first military-grade cyber weapon that can destroy pipelines and cause explosions at power plants and factories, as well as manipulate machinery. It is the first worm that corrupts industrial equipment and is also the first worm to include a PCL (programmable logic controller), software designed to hide its existence and progress. In August, security software company Symantec states that **60% of the computers infected with Stuxnet are in Iran**.

2010

August

The Pentagon declares cyberspace the "new domain of warfare."

November

Iranian president Mahmoud Ahmadinejad acknowledges that the **Stuxnet worm destroyed about 1,000 of the country's 6,0000 centrifuges at its nuclear facility** in Natanz. **Israel and the U.S. are believed to be behind the attack** in an attempt to slow Iran's progress toward obtaining nuclear weapons.

December

Anonymous attacks several businesses seen as "enemies" of WikiLeaks. The action was in response to the arrest of WikiLeaks founder, Julian Assange. In 2010, WikiLeaks provided several news organizations with hundreds of thousands of secret government and military documents about the wars in Iraq and Afghanistan, as well as cables that gave a behind-the-scenes look at American diplomacy from the perspective of high-level officials.

Cyber Warfare Milestones

2011

June

Officials at the **International Monetary Fund** report that in the previous months it had been hit by "a very **major breach" of its computer systems**. The FBI announced **evidence linking the Chinese** government to the attack.

December

Malware, named Mahdi after the Messiah in Islam, **infiltrates about 800 computers of government officials, embassy employees, and other businesspeople in Iran, Israel, Afghanistan, the United Arab Emirates, and South Africa**. The malware was embedded in email attachments and users who opened the documents were susceptible to having their emails and instant messages read by hackers.

2012

May

Flame, malware that attacks computers using Microsoft Windows, is discovered. Its development is believed to have been state-sponsored. A report, released by Budapest University's CrySyS Lab, states that "arguably, it is the most complex malware ever found." **Flame is capable of recording Skype conversations, audio, keyboard activity, network traffic and screenshots**. It is spread over a local network or USB stick. **Flame also has a kill command, wiping out all traces of it from the computer**.

May

The U.S. Department of Homeland Security announces that spear fishers have penetrated the computer systems of U.S. gas pipeline systems.

August

Hackers, who say they are Islamic and call themselves the **Cutting Sword of Justice, infiltrate the computer networks of Saudi Aramaco**, a Saudi Arabian oil company, and **wipe out the hard drives of about 30,000 computers**. Hackers left their calling card on each affected computer, displaying an image of an American flag on fire.

September

Nine banks in the U.S., including the Bank of America, Wells Fargo, and JP Morgan Chase, were hit by a distributed-denial-of-service attack that denied customers access to the banks' websites for several days. The **Islamic hacktivist group Izz ad-Din Al-Qassam Cyber Fighters (also called the Al-Qassam Brigades) takes responsibility for the attack. The group is linked to the military wing of Hamas.**

Cyber Warfare Milestones

2012 – 2013	The ***New York Times* is hacked** several times between late 2012 and early 2013 after publishing an article that investigated how members of former Prime Minister Wen Jiabao's family benefitted financially from state contracts. The hacking included gaining access to the paper's computer systems and acquiring employee's passwords. A day after The New York Times reported the incident, the *Wall Street Journal* reveals in a statement that hackers had infiltrated it, too, "for the apparent purpose of **monitoring the newspaper's China coverage."**
2013	**August 27** The *New York Times* website is shut down for about 20 hours after being hacked, allegedly by the Syrian Electronic Army, a group of hackers who back Syrian president Bashar al-Assad. The attackers accessed the site through Melbourne IT, the vendor that registers domain names.
2014	**May** **The U.S. the Justice Department unsealed an indictment of five members of Unit 61398 of the Chinese People's Liberation Army, charging them with hacking into the computer networks** of Westinghouse Electric, U.S. Steel Corp., and other companies. **Shanghai-based Unit 61398 is the cyber division of China's national army**. The move is considered largely symbolic since there is little chance the men will surrender. **July** American officials announced that **Chinese hackers had breached the computer network of the Office of Personnel Management** in March. They said they believe the hackers were targeting employees applying for top security clearances. **November** The **computer networks of Sony Pictures were hacked**, with personal medical information about employees, financial information, emails, and thousands of other documents lifted and made public. The **U.S. suspected North Korea** was behind the breech in retaliation for the upcoming release by Sony of an outlandish comedy, called *The Interview*, about a CIA plot to assassinate North Korean leader Kim Jong-un. In December, employees of Sony received threatening messages on their computers warning that "the world will be full of fear" if the film is released. "Remember the 11th of September 2001," a message said. Sony decided to cancel the release of the film. On Dec. 19, the FBI formally accused North Korea of launching the attack, saying it had significant evidence linking the government to the breech.

Cyber Warfare Milestones

2015

April

U.S. officials announced that **Russian hackers gained access to White House and State Department emails in 2014**. The emails were unclassified, but likely contained sensitive information. The hackers penetrated the email archives of White House and State Dept. officials who correspond with President Barack Obama.

June

The **White House said that the Social Security numbers and other personal identifying information of some 4 million current and former government employees** had been breached. The breach occurred in late 2014. The data was accessed from the computers of the Office of Personnel Management. The government said it believes that the hack **originated in China**.

Information cited from:

"Cyberwar Timeline"
Ask the Editors. Infoplease.
© 2000–2015 Sandbox Networks, Inc., publishing as Infoplease.
<http://www.infoplease.com/world/events/cyberwar-timeline.html>.

Recent Cyber Attacks on Businesses

- **Primera Blue Cross -** March 2015
- **Anthem -** February 2015
- **Sony Pictures -** November 2014
- **Staples -** October 2014
- **Home Depot -** September 2014
- **JPMorgan Chase -** July-August 2014
- **Community Health Systems -** June 2014
- **Michaels Stores -** April 2014
- **Target -** December 2013

Information cited from:
"9 Recent Cyberattacks Against Big Businesses"
New York Times.
<http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0>.

Recent (2016) Cyber Attack Headlines

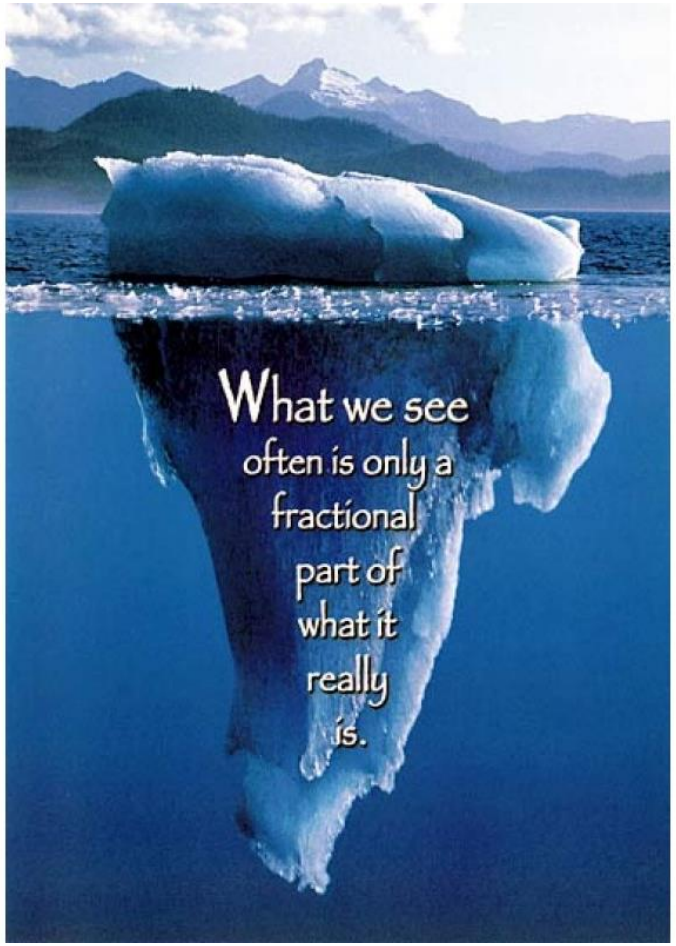
- TaxSlayer breached: 8,800 customers notified PII may be compromised [*SCmagazine.com; 1/1/2016*]
- Ukraine says to review cyber defenses after airport targeted from Russia [*Reuters.com; 1/18/2016*]
- The same group that hacked the CIA Director just took over a White House official's email [*TechInsider.io; 1/19/2016*]
- HSBC cyber attack brings Internet banking to its knees [*CNBC.com; 1/29/2016*]
- Los Angeles Hospital Hack Raises Concerns About Ransom Attacks [*NPR.org; 2/22/2016*]

Cyber Security Market Notes (*from Forbes*)

- Worldwide cybersecurity industry ranges from $75B in 2015 to $170B in 2020
- Internet of Things (IoT) security could add another $29B by 2020
- Cyber crime costs will rise from $500B in 2015 to $2T in 2019
- Ginni Rometty, Chairman, President and CEO at IBM IBM Corp. says “cyber crime is the greatest threat to every company in the world.”
- There are one million cybersecurity job openings in 2016
- U.S. News and World Report ranked a career in information security analysis eighth on its list of the 100 best jobs for 2015. They state the profession is growing at a rate of 36.5% through 2022
- Gartner IT estimates that IT security spending will soar from $75 billion-plus in 2015 to $101 billion in 2018

Observations about threat

- Has been around for awhile
- Comes from countries (friend and foe) and individuals
- Will attack anything: Defense organizations, White House, banks, airports, hospitals, research facilities, … individual assets
- Growing dramatically
- Challenges to overcome threats are huge
- We're just now starting to understand the magnitude of the threat and how to protect ourselves



SIMVENTIONS OVERVIEW

AND

CYBER SECURITY MARKET POSITION

High Level Snapshot

- ***Small business agility, big business capabilities***
  - 200+ employees (88% cleared and 54 have TS)
  - ~$38M annual revenue, steady growth since inception (‘02)
  - Certified/accredited in multiple disciplines (PM/IA/Eng)
  - Easy to contract with (Sole Source, SBSA, Full & Open)
  - Proven prime contractor (results, process, controls, & staff)
  - Workspace/business model promotes collaboration, agility, innovation, and enables interoperability
  - Our processes ensure we bring the right team at the right time and deliver on our promises

Underpinning

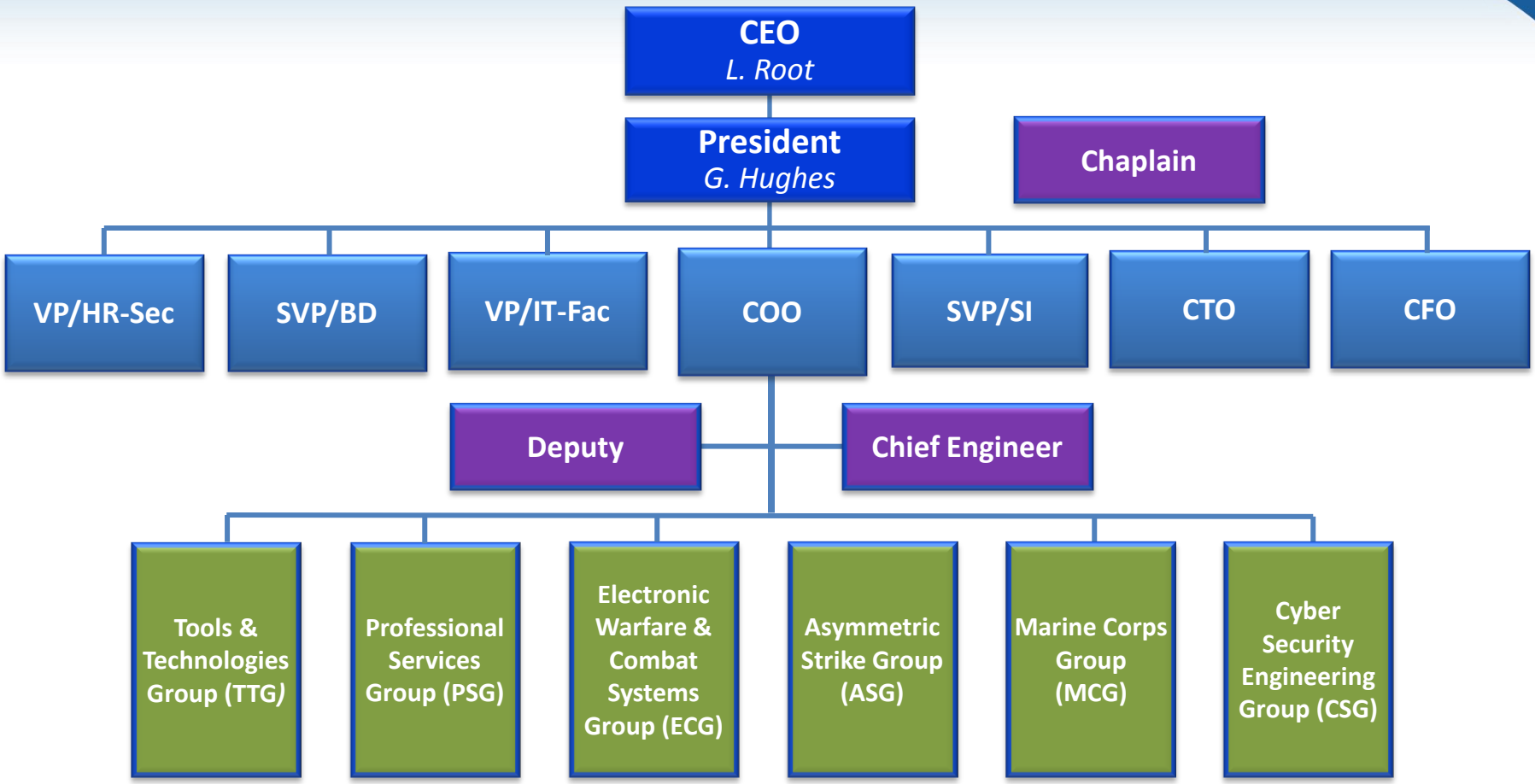
- "Imagine. Create. Explore. Discover.™" culture
- Agile, yet industry best practice/CMMI like processes
- Unparalleled retention rates, recruitment, and customer satisfaction
- Corporate core disciplines:
  - Engineering
    - Software, Systems, Security and M&S
  - Acquisition and Project Management
  - Training

- Innovative use and development of tools – created out of SBIRs and the need to better support existing customers/contracts

Facilities

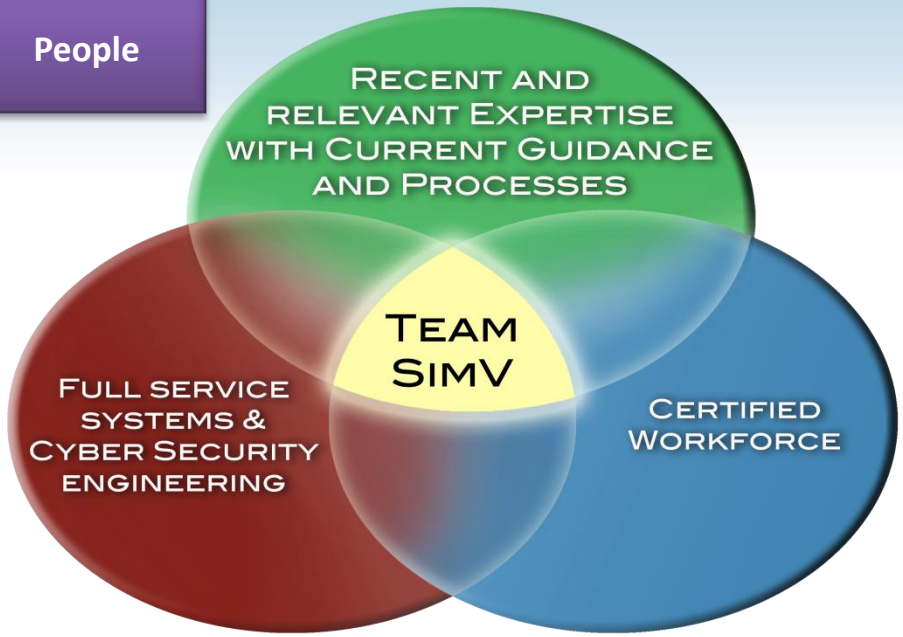
SimVentions®
Imagine. Create. Explore. Discover.™
"Your Success is Our Honor"™

Corporate Org



Cyber Security Engineering

People



Key Experience / Offerings

- Integration of cyber security engineering into systems engineering and acquisition processes
- Cyber security assessments and pen testing
- Certification and Accreditation (C&A) of systems
- Vulnerability scanning and management
- Test planning and execution
- Risk management
- Supply chain analysis
- Independent validation

Customers & Programs	Program Specifics
• Navy	End-to-end cyber security support (requirements, C&A, program reviews, working groups, testing, schedule definition, supply chain)
• Marine Corps	End-to-end cyber security support (requirements, security integration, C&A, program reviews, working groups, testing) process development for Risk Management Framework

Technology

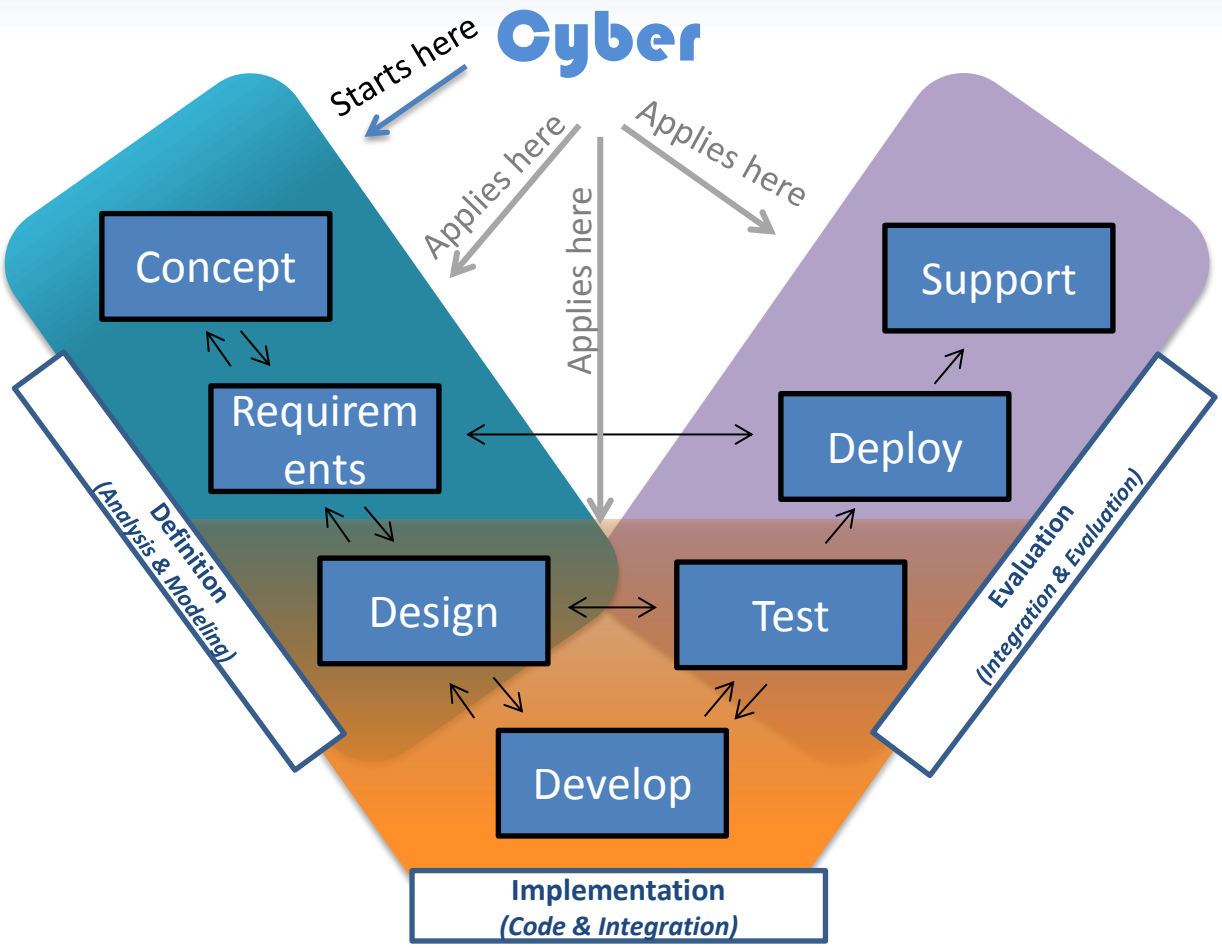
SimV Cyber Capabilities

Providing support for the entire Information Security Lifecycle

- ✓ Certification & Accreditation (C&A)
- ✓ Change / Configuration Management
- ✓ Commercial off the Shelf (COTS) Integration
- ✓ Hardware & Technology Refresh
- ✓ Identity and Access management
- ✓ Incident Management
- ✓ Business Continuity Planning
- ✓ IT Strategy & Planning Support
- ✓ Penetration Testing/Ethical Hacking
- ✓ Product Evaluations (Security Reviews)
- ✓ Regulatory Compliance
- ✓ Privacy documentation, Privacy Impact Assessment (PIA)
- ✓ Security Standards and Best Practices
- ✓ Secure network and system architecture, design, and implementation
- ✓ Network Security Posture
- ✓ Technical Requirements Analysis
- ✓ Test Plan Development & Reporting
- ✓ Verification and Validation Services
- ✓ Threat, Vulnerability, Impact, and Risk assessments

We apply the appropriate tools/technologies at the right time to support the information systems

Our View of Cyber



Cyber applies throughout the process, not just when it's time to deploy

Our Cyber Security Engineering Mission

To provide security confidence in the systems being developed / delivered and in operation by our team and for our customers.

We do this by developing and/or leveraging the technology, standards & processes, and the relevant information with the right people across the full lifecycle to provide the desire capability needed by the user

- **Technology**
- **Standards/ Processes**
- **Relevant Information**
- **People**

People

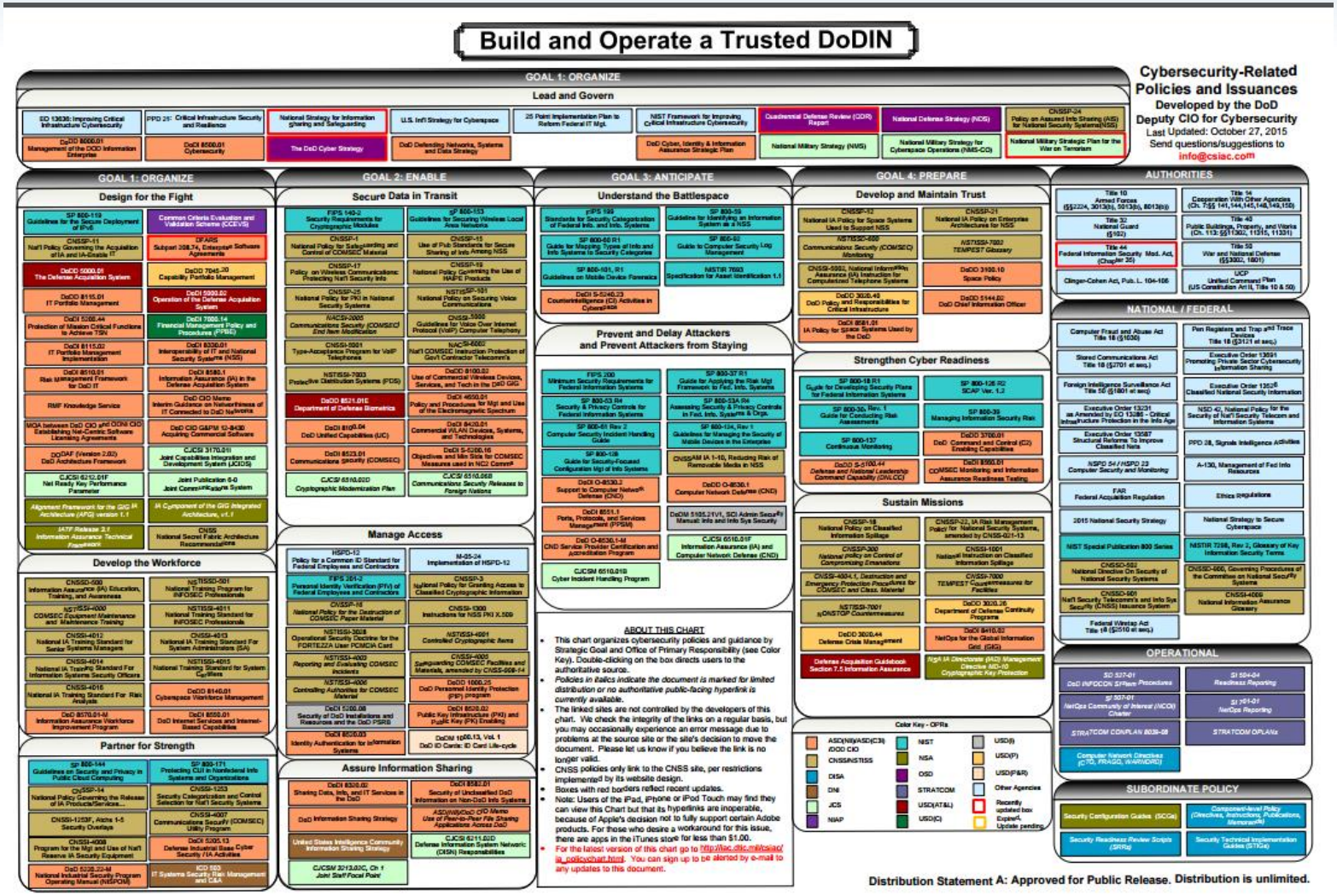
SimV Cyber Credentials

- Security + Certified Cyber Team
- EC-Council Certified Security Analyst (ECSA)
- Certified Ethical Hackers (CEH) for conducting black, gray or white hat penetration testing
- Experienced and fully qualified SimV Cyber team delivering full cycle of security solutions
- Fully Qualified Validators and Blue Team certified for conducting network and system vulnerability assessments and risk analysis
- System operators with years of cyber security and system security experience
- Certified Information Systems Security Professionals (CISSP)
- Committee on National Security Systems (CNSS) 4012/4015/4016 Certified
- COMPTIA Advanced Security Practitioner (CASP)

E|CSA™
EC-Council Certified Security Analyst

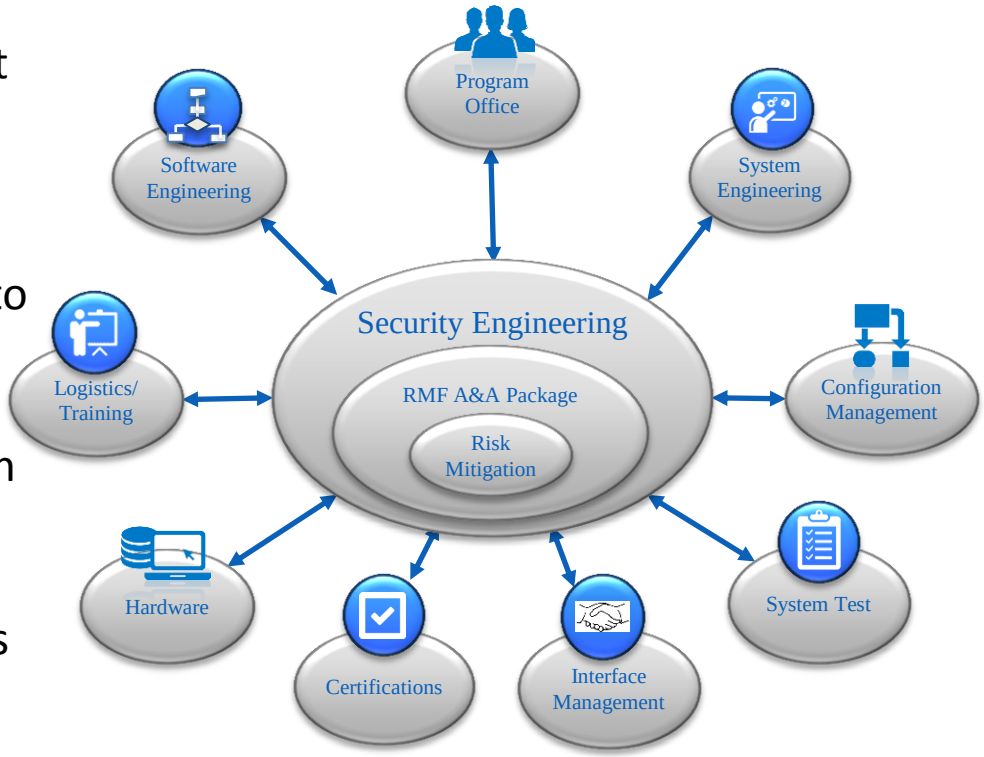
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

Cybersecurity Policy Chart



Risk Management Framework (RMF) Implementation

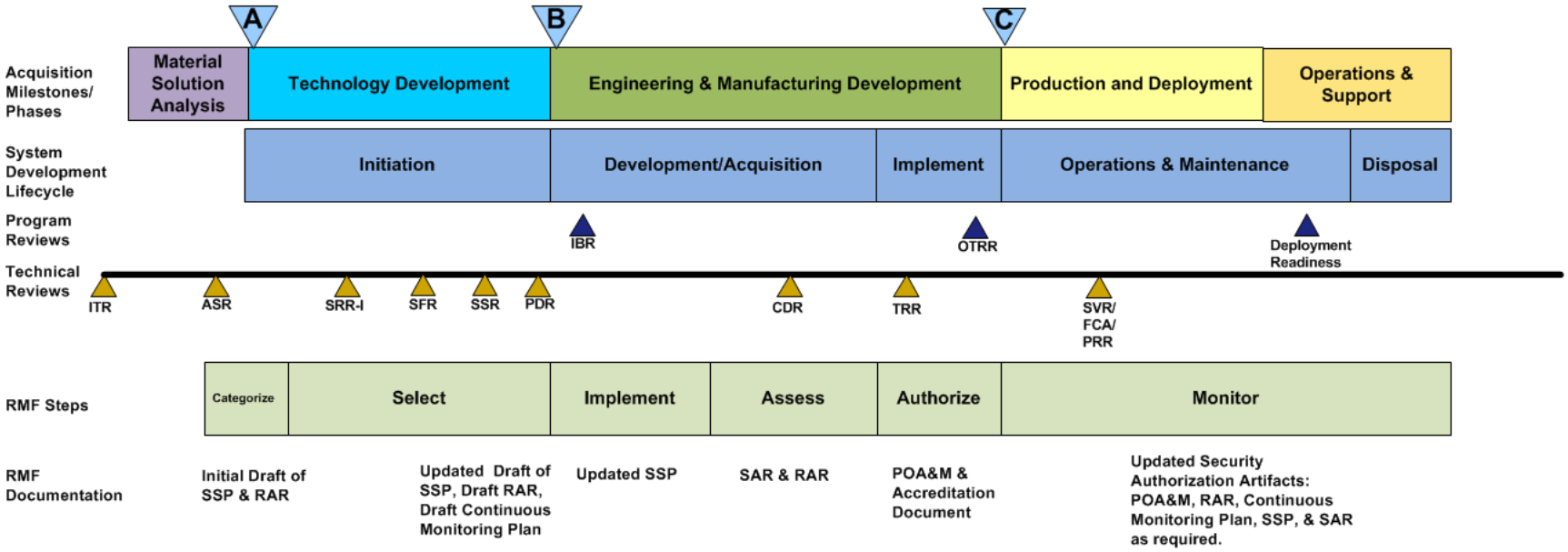
- Security team disperses relevant security controls to responsible parties
- Two-way collaboration between SMEs and security team is vital to defining measurable, testable requirements
- Risk identification and mitigation is responsibility of entire team
- Security team merges inputs from all sources to create Assess & Authorize (A&A) package artifacts, submits package and oversees the A&A process



RMF requires all stakeholders to be involved in the process. No longer is the security team responsible for security failures, but is responsible for conveying and tracking requirements.

Cybersecurity Integration

Alignment of RMF with Acquisition, SDLC and SETR Processes



Challenges in DoD

- Cybersecurity is neither understood nor embraced
- Magnitude of policy/guidance
- Alignment of policy across DoD, DON, Cyber commands, SYSCOMS, fleet, etc.
- Constant changes (technology, threats, documentation, etc.)
- Competent vs. Certified
- Not being integrated in programs
- Test Equipment/Tools (non-existent or $$$)

Stafford Technology & Research Center

- STRC concept adopted as goal by Stafford Board of Supervisors in 2010 and recently included in 2015 Economic Development 10-Point Plan
- MOUs signed with several universities and organizations
- Established initial STRC presence within Quantico Corporate Center (QCC)
- Board purchased land next to QCC for future STRC site
- → Initial Focus –Cyber Security Businesses and Technologies

How can Virginia contribute to Cyber Security Challenge?

- Support local organizations and businesses that are already in the fight
- Provide resources and “political” help to promote:
  - Advancement of cyber security technologies and solutions
  - Collaboration between cyber security organizations and businesses
  - Development of common RDT&E resources (testbeds, tools, SMEs, etc.) for companies to build and test future cyber security technologies