VERMONT

State of Vermont
Agency of Digital Services
109 State Street, 5th Floor
Montpelier, VT 05609

[phone] 802-828-4141

John Quinn III, State CIO & Secretary of ADS
Shawn Nailor, Deputy Secretary

MEMORANDUM

TO: Members of the Joint Fiscal Committee
FROM: Shawn Nailor, Deputy Secretary, Agency of Digital Services SN
DATE: July 24, 2018
SUBJECT: Vermont Security Operations Center Implementation Plan

In preparation of the Joint Fiscal Committee meeting scheduled for Friday, July 27th, please find enclosed the State of Vermont Security Operations Center (VTSOC) Implementation Plan.

Please do not hesitate to contact me if you have any questions.

State of Vermont Security Operations Center (VTSOC)

Implementation Plan

June 10, 2018

Purpose

The State of Vermont has identified the need for a security operations center (SOC). The purpose of a SOC is to have a facility or functional area that monitors, assesses, and defends enterprise information systems like web sites, databases, networks, and servers. Compromises of networks often happen in minutes and the State is not structured to identify and respond in our current configuration. A SOC contains the people, processes, and technologies to provide situational awareness of threats to information systems. A SOC also is the coordination point for any incident response involving information systems, using tactics, techniques, and procedures (TTP) to monitor for cyber security events, establishing if the threat is an actual incident, and determining the severity of the incident along with potential business impacts. Information security breaches because of malware, misconfiguration, and intrusion are costly to remediate and may affect our citizens privacy, safety, and livelihood.

Challenge

Current operations consist of analysts with duties like security system configuration, VPN changes, compliance assistance, intrusion detection monitoring at the internet boundary, and vulnerability scanning. As needed, services include incident response, IT project security reviews, security design, and policy input.

The State of Vermont does not perform active, 24/7 event and log correlation monitoring. The State does not collect logs and audit results in a centralized location and incident response is often slow while information is gathered and business unit impacts are determined before remediation can occur.

Concept of Implementation

The State of Vermont, Agency of Digital Services (ADS) plans to collaborate with Norwich University to create the Vermont Security Operations Center (VTSOC). The broad concept is that Norwich will create the physical facilities, host the monitoring systems and software, and staff the monitoring with a mixture of full-time professional security analysts and students from its Cyber Security Program. Norwich is uniquely qualified for this mission due to their proximity to Montpelier, their cybersecurity apprenticeship program, and other ongoing initiatives with the State like internship programs and network assessment exercises (more information is available in Attachments A and B). The State of Vermont will provide network security sensor logs and other log data to Norwich and will have trained personnel to respond to any events identified through Norwich's monitoring facility.

The initial implementation will use a phased approach. Using the premise of plan, design, build, operate, and review, Norwich and the State will develop the foundations for a SOC in parallel. As the phases progress, Norwich and ADS will begin to merge functionality and coordinate more closely, culminating in a unified effort by Phase 4.

Phase 1 (Norwich): Norwich will define the problem and scope the VTSOC's critical functions, capabilities, and costs with ADS. The VTSOC program leverages standing Norwich University Applied Research Institute (NUARI) partnerships and programs to create a nationally networked cyber threat intelligence system (see Attachment B). This phase will also research each proposed line of operation like staffing levels, threat analysis functionality, and the cyber security apprenticeship program to establish a comprehensive, sustainable, and cost-effective VTSOC program. July/August 2018

Phase 1 (ADS): ADS will recruit and place an analyst to coordinate and respond to cyber security incidents. This analyst will also work closely with Norwich to provide a link between ADS leadership and Norwich while they plan and scope the VTSOC. The analyst will be vital to defining the critical functions that will encompass our VTSOC. Last, ADS will identify staff training requirements and schedule those individuals for training. July/August 2018.

Phase 2 (Norwich): Norwich will design and initiate the creation of the VTSOC systems and structure and will work with ADS to schedule the stand-up of the facility. This phase will trigger the selection of a security information and event manager (SIEM). Norwich will also use this phase to establish national program linkages and coordination proposals. September – December 2018.

Phase 2 (ADS): ADS will use this phase to order the network security sensor equipment and incident response equipment. Staff training will commence during this phase to ensure personnel have the proper training and are ready to support the initiation of the VTSOC. The SOC analyst and ADS leadership will collaborate with Norwich to provide guidance regarding systems and structure. September – December 2018.

Phase 3 (Norwich): Norwich will establish the physical center at Norwich University and be at initial operating capacity. Activities during this phase include recruitment of initial full-time staff and students to fulfill critical threat analyst roles in the VTSOC. This phase will also establish staff and student training, initial standard operating procedures (SOP), policies, technology solutions (hardware and software) and initial connections to state, local, and national partners to include MS-ISAC, DHS, NCCIC, and USCERT. January – March 2019.

Phase 3 (ADS): ADS staff will participate in coordinated training events to build a cohesive team concept with the Norwich staff. ADS will provide input to the SOP and collaborate and assist Norwich with establishing the national partnerships. This phase will also be when ADS coordinates with MS-ISAC to incorporate their member services to extend the State's capability in cyber incident response and forensics investigation. January – March 2019.

Phase 4 (Norwich and ADS): Norwich and ADS will establish full operational capacity of the VTSOC. Full operation is defined as the VTSOC delivering services and threat warnings and being fully staffed and trained. April – June 2019.

Milestones and Timeline

Phase 1: July 1 – August 30, 2018. Report delivered by Norwich; ADS will have new analyst in place and a training plan and schedule prepared by September 1, 2018.

Phase 2: September 1 – December 30, 2018. Norwich will deliver the plan for the VTSOC creation with supporting material; ADS will have staff training complete and equipment ordered by January 2, 2019.

Phase 3: January 2 – March 30, 2019. VTSOC will be at initial operating capacity and Norwich and ADS will have agreements in place with extended partners by April 1, 2019.

Phase 4: April 1 – June 30, 2019. VTSOC to full operational capacity, first year assessment complete and year two plan delivered to ADS Secretary by June 30, 2019.

Budget and Expenditures

Item	Description	Phase 1 9/1/18	Phase 2 1/2/19	Phase 3 4/1/19	Phase 4 6/30/19	Total
Norwich Contracting	Labor and materials	$15,777	$81,487	$126,181	$176,219	$399,664
Training	ADS staff training for proficiency	-	$25,830	$6,210	-	$32,040
Equipment	Incident response (IR) kit	-	$6,500	-	-	$6,500
Equipment	Network security sensors	-	$153,600	-	-	$153,600
Total by Phase		$15,777	$267,417	$132,391	$176,219	$591,804

Supporting breakdown of expenditures

IR kit contains a custom laptop, write-blocker drives, forensic license software, toolkit, storage drives, and a case for portability. Cost is $6,500.

The training budget total is $32,040, consisting of:

SANS Incident Response and Forensic Courses

- SEC503 – Intrusion Detection in-depth: 3 seats at $6,210/ea. for a total of $18,630
- FOR500 – Windows Forensic Analysis: 1 seat at $6,210/ea. for a total of $6,210

Elastic Training courses (backend to most SIEM)

- Elastic Engineer I – 2 seats at $1,800/ea. for a total of $3,600
- Elastic Engineer II – 2 seats at $1,800/ea. for a total of $3,600

The BRO network security sensors: Total $153,600

- AP1000 (10G) – 2 at $48,000/ea. for a total of $96,000
- AP200 (2G) – 6 at $9,600/ea. for a total of $57,600

Norwich Expenses

- Labor - $316,745
  - Program Manager - $46,266
  - SOC manager - $79,617
  - Cyber Apprentices - $43,215
  - Cyber SME - $83,100
  - Threat Intel Lead - $45,529
  - System Admin - $19,018
- Direct Costs (materials, travel, etc.) - $82,919

Using Norwich as a sole-source vendor will deepen our ties with an educational institution that provides significant benefit in workforce development, national partnership connections, and leverages Norwich's Information Sharing and Analysis Organization (ISAO) initiative.

The SIEM cost is rolled into the implementation for the first year. This expense will likely increase as we move into year two. As year one progresses, ADS will work with Norwich to understand the expenses involved in an ongoing relationship and plan accordingly based on a balance of cost, benefit, and information systems risk.

Metrics

ADS plans to keep statistics as the VTSOC comes on line both initial and full operational capacity. The first group of statistics will center around the performance of the VTSOC systems and personnel:

- Number of personnel hours to maintain analysis and notification
- Amount of log files received
- Number of log files reviewed
- Number of events identified

The second group of statistics will speak to the performance of the personnel and the efficiency of the VTSOC:

- Number of events analyzed
- Number of events converted to incidents
- Mean time to resolve incidents
- Number of incidents referred to another source for further analysis

The purpose of gathering these statistics is to set a baseline. ADS leadership, Norwich University, and State VTSOC personnel will determine metrics to achieve based on the baseline and the capacity to handle the incidents identified.

Terminology and Technology

SIEM – system that aggregates and correlates data from security feeds such as network discovery and vulnerability assessment systems. The SIEM may also accept feeds from threat intelligence systems, network security sensors, and intrusion detection systems.

Network security sensors – create visibility by turning network traffic and patterns into data. Sensors are typically placed at key junctions in the network where they can monitor access and flow to critical systems. These sensors are sized to fit the volume of network traffic where they are placed.

Intrusion detection systems - a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically either reported to an administrator or collected centrally using a SIEM system.

Threat intelligence – evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. A threat intelligence system is typically tied in to multiple, vetted data sources and provides a data feed to a SIEM or other log aggregator.

Vulnerability scanning - an inspection of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks, and communications equipment and predicts the effectiveness of countermeasures.

Incident Response - an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident, or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

MS-ISAC – Multi-State Information Sharing and Analysis Center

DHS – Department of Homeland Security

NCCIC – National Cybersecurity and Communications Integration Center

USCERT – United States Computer Emergency Readiness Team

Supporting information for Norwich University.

Member of the National Cybersecurity Preparedness Consortium – http://nationalcpc.org/
The NCPC has been awarded FEMA Continuing Training grants since 2014 providing cybersecurity training and education nationally. Please see attached brochures. Norwich has been the prime on grants awarded in FY2014 and FY2017 with total funding in the past 5 years in excess of $5.0M

Norwich has developed DECIDE a cyber security exercise platform used in the financial sector to test and evaluate sector playbooks, coordinate critical partner actions, and organizational readiness to cyber security events. DECIDE was used by 14 institutions on June 13, 2018 to test the newly FSARC developed Treasury Market Playbook. DECIDE has been used by most of the largest US banks and systemically significant financial institutions to test and develop response and recovery plans in the past 12 months.

Norwich operates the Global Threat Observatory a student operated and faculty mentored environment collecting netflow data from 38 sensors embedded in partner institutions. The data is analyzed with a variety of professional tools. Students use the data to develop new tools, practice and develop visualization, and develop greater understanding security operations center operations. The Global Threat Observatory was used to support Super Bowl 50 and is contracted to support the Collegiate National Championship in 2019.

Norwich was a founding member of the Army Reserve Public Private Partnership providing Cyber Security Scholarships to Army Reserve members.

Norwich has cyber security past performance with US DOD and SOCOM for the development of tools, techniques and procedures associated with exploitable vulnerability analysis. Norwich provided test and evaluation services for multi-level security software and presently under contract to assist in developing the inter-change data format for emerging soldier fielded augmented reality systems.

Presently Norwich is working with Colorado – National Cyber Exchange and University of Colorado, Colorado Springs and Public Infrastructure Security Collaboration Exchange System, PISCES and University of Washington to develop a national pilot Information Sharing Initiative. The concept is to deliver cost effective monitoring solution using students at NSA Centers of Academic Excellence to provide coverage; the students gain skill and experience. The students are mentored by professionals in a Security Operations Center model.

2011

Norwich University receives U.S. Department of Defense Cybercrime Center of Digital Forensic Academic Excellence **(CDFAE)** designation for the first time.

NUARI runs **Quantum Dawn I,** the largest critical infrastructure cyber threat exercise with the financial sector at the time.

CDFAE

2009

NU Center for Advanced Computing and Digital Forensics (NUCAC-DF) is created.

NUARI and U.S. Senator Patrick Leahy, D-VT, announce a $15 million contract, of which $6 million is awarded through the Air Force Research Lab in Rome, NY, to fund research to develop Web*DECIDE, a war gaming platform for the financial sector.

NUCAC-DF

2002

The National Center for the Study of Counter-Terrorism and CyberCrime at Norwich University (later **NUARI**) is funded through a U.S. Department of Justice grant.

NU enters the NSF Cyber Corps.

CGCS launches online **Master of Science in Information Assurance Program** (later became MSISA).

NUARI & MSISA Launch

2001

The NSA designates Norwich University as a **National Center of Academic Excellence in Information Assurance Education** (CAE-IAE) for the first time.

CAE-IAE

1999

Bachelor of Science in Computer Security & Information Assurance (BSCSIA) program launches. Based on theory and hands-on experience, the program utilizes state-of-the-art forensic tools, today offering concentrations in Advanced Information Assurance and Digital Forensics.

BSCSIA

NORWICH UNIVERSITY CYBER TIMELINE

2017	CAE-CDE & CDFAE
2016	MSISA Ranked #3
2015	Online BSCS Launch
2014	NU Programs Ranked #2
2013	DHS
2011	CDFAE Designation
2009	NUCAC-DF is created
2008	Norwich University collaborates with top officials at Federal agencies and the U.S. Department of Defense on cybersecurity exercises.
2003	
2002	NUARI & MSISA Launch
2001	CAE-IAE Designation
1999	BSCSIA Launches

CYBER AT NORWICH

Bachelor of Science in Computer Security & Information Assurance

Concentrations in Advanced Information Assurance or Digital Forensics

Bachelor of Science in Cyber Security

(online degree completion program)

Concentrations in Computer Forensics and Vulnerability Management or Information Warfare and Security Management

Graduate Certificates in Information Security & Assurance

(online programs)

Four certificates available

Master of Science in Information Security & Assurance

(online program)

Five concentrations available

NORWICH UNIVERSITY®
1819
Expect Challenge. Achieve Distinction.

158 Harmon Drive, Northfield, VT 05663 • (802) 485-2080 • *www.norwich.edu*

NORWICH UNIVERSITY CYBER TIMELINE

2017

For the third year in a row, Norwich receives a grant from the National Security Agency (NSA) and National Science Foundation (NSF) to host **GenCyber@NU**, a free cybersecurity camp for high school juniors and seniors.

Norwich University is named a **Center of Academic Excellence in Cyber Defense Education** (CAE-CDE) by the NSA and Department of Homeland Security (DHS) through 2022. The Department of Defense (DoD) Cyber Crime Center certifies Norwich as a **National Center for Digital Forensic Academic Excellence** (CDFAE).

College of Graduate and Continuing Studies (CGCS) holds the inaugural **Cybersecurity Summit** bringing leaders together to discuss the latest in federal cyber policy.

CAE-CDE & CDFAE

2016

The Norwich Bachelor of Science in Computer Security & Information Assurance (BSCSIA) program was the only educational institution invited to support Santa Clara Police Department at **Super Bowl 50.**

Norwich's Master of Science in Information Security & Assurance (MSISA) is ranked #3 in the top 10 best cybersecurity graduate programs in the U.S. by *Universities.com.*

Norwich University Applied Research Institutes (NUARI) deploys DECIDE-FS software simulation in South Africa, facilitating a cyber-resiliency response exercise with 16 institutions integral to its **financial markets.**

Norwich launches inaugural **Cybersecurity Awareness Month** in October.

Norwich awarded NSA grant to train the next generation of cyber soldiers, awarding scholarships to U.S. Army Reserve soldiers to enter the online Information Security & Assurance certificate programs.

MSISA Ranked #3 in the U.S.

2015

Online Bachelor of Science in Cyber Security (BSCS), a degree completion program, launches at CGCS.

The 20th Anniversary **William E. Colby Military Writers' Symposium** addresses the theme of cyber security and privacy.

NU is one of six universities **in the U.S. to officially partner with the United States Army Reserve** to develop cyber-education curricula that aligns with federal standards and cybersecurity needs.

The **302nd Information Operations Battalion Web OpSec detachment,** a United States Army Reserve detachment, forms on the Norwich campus.

NUARI runs **Quantum Dawn III** simulation with over 80 financial institutions and government organizations in the largest financial sector cybersecurity exercise in the U.S.

Online BSCS

2014

Norwich rated number two for its cyber security academic programs in the U.S. by the **Ponemon Institute** in a survey of nearly 2000 information security professionals assessing 403 colleges and universities.

NU Programs Ranked #2 in U.S.

2013

U.S. Senator Patrick Leahy, D-VT, announces a **$9.9 million Homeland Security contract** to NUARI to continue work on DECIDE simulation software.

NUARI runs **Quantum Dawn II** with 50 organizations and 500 participants in the financial sector. At this time, it is the only cyber threat exercise of its kind.

DHS

NORWICH UNIVERSITY

CSIA is one of the most popular undergraduate majors.

CSIA graduates have gone on to careers at NSA, DHS, DoD, Booz Allen Hamilton and in federally-funded research, among others.

Many students get job offers before they graduate.

There are over 1006 MS in Information & Security Assurance alumni.

www.norwich.edu

National Network State Information Analysis Organization (ISAO) Pilot Program

Justification: the nature of the cybersecurity threat to America is growing, and our nation's cyber adversaries move with speed and stealth. To keep pace, all types of organizations, including those beyond traditional critical infrastructure sectors, need to be able to share information and respond to cyber risk in as close to real-time as possible. Organizations engaged in information sharing related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States.

Responding to this challenge for Private Sector Cybersecurity Information Sharing, three states spanning the geographical boundaries of the United States have come together to propose a (Integrated Public/Private or) non-governmental pilot program for information sharing in which each state will develop the full capability to perform information sharing and analysis of cybersecurity threats. The three organizations, each comprised of partnerships of State Government, University, Non-Profit Research and Private Sector organizations, will engage public and private sector organizations to meet the cybersecurity crisis. The success of this proposed National Network of State ISAOs (N2SI) is the idea of local, state trust-based threat and incident information sharing capabilities that can network nationally facilitating tactical to strategic integration. Each state based non-profit will establish a constituency and will develop partnerships, private and public, for the purpose of sharing alerts and threat information, making all levels aware of the severity of the threat, training and educating the workforce, and conducting research and development. Thus, the N2SI team will create regional ISAOs to gather, analyze, and disseminate critical infrastructure information, for the expressed purpose of:

- Cyber threat analysis and information sharing

  Education and training to develop a cyber-capable workforce
- Technical research and development to support effective information sharing
- Shared best practices

It is the intent of the N2SI proposal to leverage what already exists: the N2SI effort will develop regional centers whose primary function is Cyber Threat Analysis and Information Sharing, workforce development, and best practice to engage the State and Local organizations. Each organization will develop a collaboration including higher education, STEM K-12, industry, not-for-profits, and government outreach. These N2SI cross-sectional collaborations will facilitate the development of trust- based relationships which are essential for effective and efficient information sharing. The N2SI centers will be guided by the requirement of ISAO best practices: inclusive, actionable, transparent, and trusted.

The objectives of the program include:

1. Establish a fully functional ISAO within each of the participating states: Colorado, Vermont, and Washington.

2. Develop a Joint Cyber Threat Exchange (CTX) platform built on the National Cyber Exchange and develop relationships with MS-ISAC, NCCIC, and other entities to allow real time or near-real time sharing of cyber threat information between ISAOs.
3. Provide the ability to provide an opt-in ad-hoc committee(s) across the ISAO network to address real-time threat events.
4. Develop the policy and procedures to provide escalation to law enforcement, Department of Homeland Security, and to national security within a regional activity and awareness across the network.
5. Develop hands-on work force development programs in collaboration with academia.
6. Develop documentation including design, policies and procedures, CONOPS, and operations manual(s),
7. Academic partners will utilize operations centers to provide real world learning environments to improve student skills and identify research opportunities for students and faculty to explore the full spectrum of cyber technology.

Each state will maintain an ISAO to allow for the reception of and secure storage of cyber threat information and artifacts, analysis programs and platforms, and interconnectivity with the other states.