National Cybercrime Investigators Program

HANDBOOK FOR THE

NCIP CYBER INVESTIGATIONS PROGRAM

June 2021

Sheriff David Goad
Dennis Kelly, Esq.
Editors

info@ncip.tech 504-717-4872
www.NCIP.tech www.e-Ponte.tech

National Cybercrime Investigators Program

HANDBOOK FOR THE
NCIP CYBER INVESTIGATIONS PROGRAM
JUNE 2021

TABLE OF CONTENTS

National Cybercrime Investigators Program

HANDBOOK FOR THE
NCIP CYBER INVESTIGATIONS PROGRAM
JUNE 2021

INTRODUCTION

This Handbook provides operational details needed to implement the NCIP Cyber Investigations Program ("Program"). This Program began with the 2017 request of the leadership of the National Sheriffs' Association (NSA) Homeland Security Committee that Sheriff David Goad, 2008-09 NSA President, form a work group to chart a path forward for Sheriffs, Municipal Police Chiefs, and NSA on how they should address the critical issues of cybersecurity and cyber crime.

In response, Sheriff Goad formed the NSA Cybersecurity & Crime Work Group ("Work Group"), which, between 2017 and 2021, has held more than 50 monthly meetings, has developed and launched the National Cybercrime Investigators Program ("NCIP), see www.NCIP.tech and www.e-Ponte.tech, has regularly reported to the Homeland Security Committee on its progress, and has spoken for the interests of Sheriffs and NSA in engaging with **IACP Committees,** the **Uniform Law Commission,** the **Paris Call for Trust and Security in Cyberspace** and others. Recognizing this progress, the NSA adopted NSA Resolutions of Support in 2018 and 2019.

Cyber-Enabled Crimes v. Cyber-Native Crimes

> **"Cyber-enabled crimes are traditional crimes that now have a new mode for delivery. They might be committed online, though social media, or through cell phones, but they're still traditional crimes."**
>
> **"Cyber-native crimes are those that can only be committed because we have these [Internet] tools. They didn't necessarily exist as crimes before these tools were available."**

Ravi Satkalmi, Deputy Director for Intelligence Analysis, NYPD

From inception, NCIP has been focused on assuring law enforcement personnel access to free/low-cost training on investigating cybercrime. Initially focused on technical training, NCIP's training ambition has considerably expanded by virtue of the results of the NYPD Cyber Investigative Standards Pilot Program, which found an important investigative distinction between "Cyber Enabled" crimes and "Cyber Native" crimes. **NCIP's ambitions now include non-technical training for large numbers of non-technical officers dealing with "Cyber Enabled" crimes, and for large numbers of technical SMEs investigating "Cyber Native" crimes, especially by the FBI Regional Computer Laboratories (RCFLs)—both at no charge to law enforcement.**

This Handbook provides high-level explanations of each of the elements of the NCIP Cyber Investigation Program, as well as complete or sample copies of key documents. More complete documentation is available at the Investigations Overview, Cyber Enabled Crimes, Cyber Native Crimes and NCIP FORUM & NCIP ISE tabs of the www.e-Ponte.tech website.

Many Sheriffs and Chiefs are already investigating "Cyber Enabled" crimes, and this Handbook provides new tools for them to standardize and formalize that process, and to expand into "Cyber Native" investigations when the time is right.

TAB A

ABOUT NCIP'S CYBER INVESTIGATIONS PROGRAM

In many ways, the direction of NCIP's Cyber Investigations Program reflects the lessons learned, and the path blazed, by NYPD in its efforts to fulfill its law enforcement charter and organizational mandate to meaningfully respond to constituent complaints of "Cybercrimes".

That is, NYPD launched its NYPD Cyber Investigative Standards Pilot Program, and, in the process, found that the term "Cybercrime" is overbroad and confusing, from an investigative perspective. NYPD also developed the understanding of the "cybercrime" problem that, from an investigative perspective, many "cyber" cases could be investigated and cleared using traditional policing methods and processes, without any meaningful technical "cyber" knowledge, while other cases require deep technical "cyber" knowledge in order to be cleared. Concluding that the term "Cybercrime" should be replaced with less confusing terminology, NYPD coined two new terms for these two types of cases: "Cyber Enabled Crimes" and "Cyber Native Crimes".

Here's what these two terms refer to:

- **Cyber Enabled Crimes** are traditional crimes abetted by cyber tools (e.g., **fraud, scams, larceny, grand larceny, and extortion**); or facilitated by use of cyber tools, like coordination or planning of traditional crimes using digital devices like phones or computers. Cyber Enabled cases, then, can be investigated and cleared using traditional policing methods and processes, without meaningful technical "cyber" knowledge.
- **Cyber Native Crimes**, on the other hand, are crimes (like **cryptocurrency hacking, network intrusion, election tampering** or **data theft**) that could not be committed outside the digital domain. Cyber Native cases require deep technical "cyber" knowledge in order to be cleared.

NCIP's Cyber Enabled Investigations Program, then, is based on the "lessons learned" by NYPD in developing its understanding of Cyber Enabled Crimes, and is executed using the SCIO App and SCIO App Training provided to law enforcement agencies at no charge.

NCIP's Cyber Native Investigations Program, on the other hand, is based on two NCIP initiatives.

- One involves separating the efforts required to conduct a Preliminary Investigation of a Cyber Native case, from the efforts required to fully investigate such a case. The premise here is that a Preliminary Investigation of a Cyber Native case can be accomplished by a Level 1 (or higher) Cyber Investigator, while a full investigation will typically require considerably more technical cyber expertise. This initiative has been accomplished by NCIP's creation of the Incident Data Report Documents, completion of which concludes the Preliminary Investigation Phase of a Cyber Native Investigation.
- The second initiative is to standardize the collection and sharing of information about Cyber Native incidents using the Incident Data Report Documents, because sharing that information will be useful to many other investigations, even if the investigation of the originating case is not completed.

Both of these NCIP programs comply with authoritative guidance in NIST SPECIAL PUBLICATION 800-61, REV 2, "Computer Security Incident Handling Guide", and are based on cybersecurity industry best practices.

Guide to Conducting Cyber Investigations Using NCIP Tools

Guide For Sheriffs and Chiefs to Conduct Cyber Investigations Using NCIP Tools

NSA Annual Conference, June 2021

About NCIP

- Mission: provide pre-packaged tools and a clear path forward for Sheriffs & Chiefs to investigate & prosecute cybercrimes and share info nationwide
- Launched by NSA Cybersecurity & Crime Work Group at the Instance of NSA Homeland Security Committee
- NSA Resolutions of Support, 2018 & 2019
- A Reporting Program of the Emergency Services Sector Coordinating Council
- Supported by e-Ponte Foundation, a 501(c)(3)
- Chaired by Sheriff David Goad
- Subject to Oversight of NCIP Executive Committee
- Partners with Cybercrime Support Network, NYPD and Others to provide No Cost/Low Cost Training, Investigation & Info Sharing Tools

NCIP & NCIP Partner Tools For Law Enforcement For Cyber Enabled & Cyber Native Investigations

- **Cybercrime Victim Support**, provided by Cybercrime Support Network*
- **NCIP Train-The-Trainer Training**, Provided by NCIP & NYPD*
- **Cyber Enabled Crime Investigation Support,** Provided by Agency Trainers*
- **NCIP Cyber Investigation Training**, Materials provided by NCIP, NYPD and Nick Selby *
- **The SCIO App**, Provided by NCIP courtesy of NYPD, Nick Selby & Raven Zachary*
- **NCIP Incident Data Reports (multiple)**, provided by NCIP*
- **NCIP-Standard Playbooks (multiple)**, as selected by NCIP*
- **NCIP Forum Information Sharing Environment,** Provided by NCIP and NCIP Forum**

* No Law Enforcement Charge **Nominal Charge ***Professional Services provided as Contracted

Tools Provided to Law Enforcement for No or Nominal Charge

*No charge for Cybercrime Victim Support, provided by Cybercrime Support Network

*No charge for Training & Training Materials

*Service Request Forms provided at no charge; CFL Services are as quoted and agreed

***SCIO App** provided at no charge to Law Enforcement Agencies

****NCIP Forum** provided to Law Enforcement Investigators for a nominal charge

To Prepare to Respond to Cybercrime Complaints

- Your agency’s **Chief of Investigations** or other responsible leader implements the following agency roles:
  - The agency’s **Chief Training Officer** designates non-technical **NCIP Cyber Investigation Trainers (“Trainers”)** for **Roll Call Training** and requires agency **Trainers** to complete **NCIP Train-The-Trainer Training;**
  - The agency’s **Chief Training Officer** institutes **Cyber Investigation Training** as periodic **Roll Call Training** for all **Patrol** and **other non-technical personnel dealing with the public**, including **Records Management System (RMS) Intake Personnel;**
  - The agency’s **Chief of Investigations** designates one or more investigators as **Cyber Detectives,** who enroll in the **NCIP Forum Information Sharing Environment**.

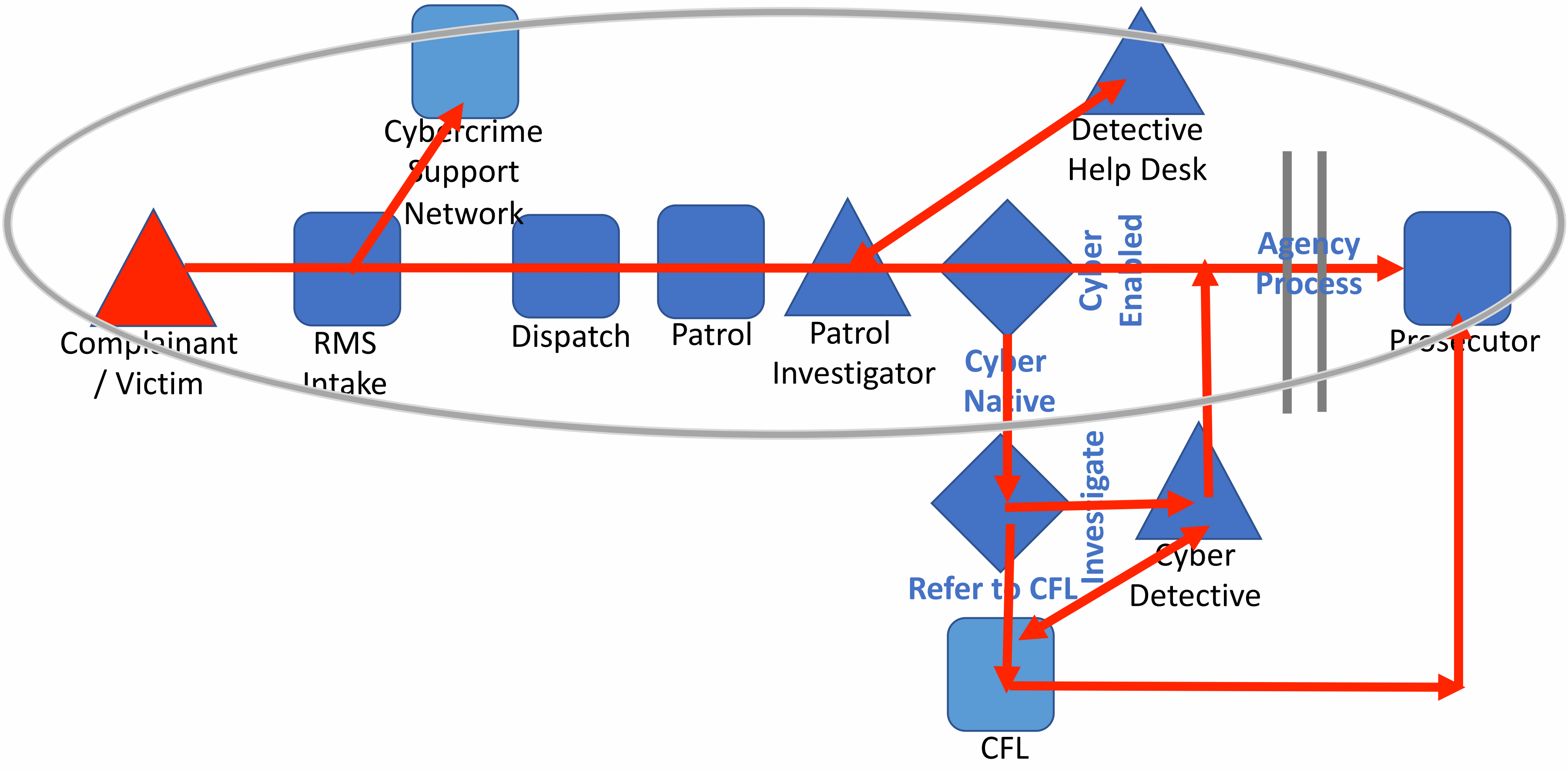
To Respond to Cybercrime Complaints

- **RMS Intake Personnel**:
  - Refer the victim to the **Cybercrime Support Network** for **Cybercrime Victim Services**;
  - Connect the victim with **Dispatch** for **Patrol Investigation** by the **Patrol Division**;

To Investigate Cyber Enabled Crimes

- after determining that the complaint concerns a **“Cyber Enabled” crime**, the **Patrol Investigator**:
    - Works with the Victim/Complainant to answer the questions presented by the **Cyber Enabled App**;
    - Sends the **Cyber Enabled App’s** Report to CFL for info sharing and review by an experienced **non-technical Detective** to develop, with the **Patrol Investigator**, an investigative plan for the Cyber Enabled Complaint.

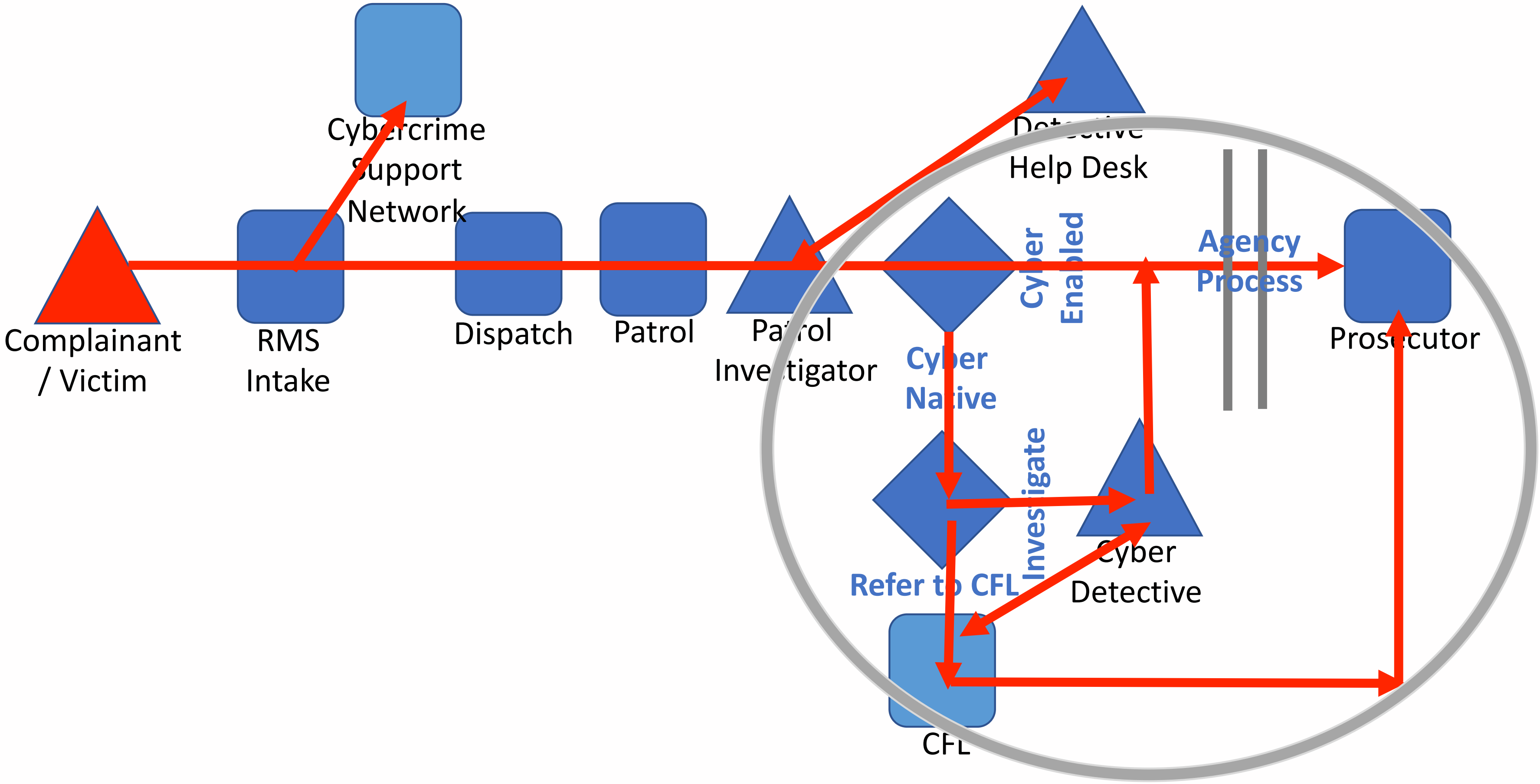
Cyber Enabled Investigation Process



To Investigate Cyber Native Crimes

- after the Patrol Investigator determines that the complaint concerns a **“Cyber Native” crime**,
  - the **Patrol Investigator** refers the complaint to the **Cyber Detective Bureau**, who assigns a **Cyber Native Detective** and a **Cyber Native Intake Specialist**, who works with the victim/complainant to complete one of the following: an **NCIP CFL Form 1—Forensic Service Request**; an **NCIP CFL Form 2—Intrusions Laboratory Request**; or an **NCIP CFL Form 3—Digital Media Recovery Laboratory Request**, or the appropriate form on the **Cyber Native App**, when available;
  - The **Cyber Native Intake Specialist** submits the applicable **NCIP CFL Service Request Form** to the assigned **Cyber Native Detective** for review and action;
  - If there is an agency decision to conduct an in-house investigation, it is handled by the assigned **Cyber Native Detective** using the **Cyber Native App**;
  - However, if the agency decides to request an evaluation and quote from the NCIP CFL, the **NCIP CFL Service Request Form** is submitted to the NCIP CFL for an evaluation and quote, and the investigation proceeds.

Cyber Native Investigative Process



As the Prosecution Trial Date Approaches

prosecutors may request Litigation Support from NCIP CFL by submitting **NCIP CFL Form 4—Litigation Support Request or** using the **Cyber Native App**.

Questions

Sheriff David Goad, CEO, NCIP

301-268-2901

dgoad@NCIP.tech

Dennis Kelly, Esq., Secretary & General Counsel

504-251-0240

dkelly@NCIP.tech

Info@NCIP.tech 504-717-4872

www.NCIP.tech www.e-Ponte.tech

TAB B

ABOUT THE NCIP INFORMATION SHARING ENVIRONMENT (ISE)

From its inception, NCIP has placed high priority on providing local law enforcement with a robust information sharing environment, in order that investigators may realize the force multiplier efficiency and effectiveness benefits of information sharing. As background, some Members of the FBI Cyber Squad have advised that the information sharing environment they use for Cyber Squad investigations is their single most important tool in their toolbox for efficiently and effectively conducting cybersecurity incident investigations.

NCIP is grounded upon recognition of the realities of the overwhelming cyberthreat, law enforcement resource constraints and the multi-jurisdictional nature of cybersecurity incidents. NCIP is also aware that many Federal law enforcement agencies, and some State, local and University law enforcement agencies, have developed and proven successful cybersecurity incident investigative practices built on collaboration and information sharing between law enforcement agencies and between law enforcement/non-law enforcement cyber investigation/critical infrastructure firms.

NCIP is focused on bringing the benefits of cross-jurisdiction and cross-sector collaboration and information sharing to local law enforcement, utilizing ISE technical security designs and measures to limit ISE access to trusted users and to enable law enforcement agencies to control the information they share and to limit the information they receive.

To serve a platform aimed at succeeding at facilitating collaboration and information sharing, NCIP has established a process for vetting and certifying law enforcement agencies and cyber investigation firms judged to be trustworthy. Based on a derivative trust model, NCIP then certifies investigators nominated by trusted agencies and firms, principally based on assurances received by the nominating agency or firm. Forms for law enforcement agency and cyber investigation firm applications for their NCIP certification, and for their nomination of their investigators for NCIP certification are attached.

Recognizing the cost of creating and maintaining any Information Sharing Environment, NCIP has recognized that no NCIP Information Sharing Environment will be sustainable unless it is built on a Software-As-A-Service (SAAS) service model. All NCIP ISE's are expected to be provided under the SAAS service model, with law enforcement users paying relatively nominal sustainment user fees.

The NCIP FORUM is the first element of the NCIP ISE. Documents attached describe the FORUM.

NCIP anticipates that, over time, as NCIP and users gain more investigative experience, the Forum's functionality will be further enhanced and that additional applications will be implemented to collect and share investigative information and to automate cybersecurity incident investigative processes, just as private sector cybersecurity incident investigators have begun automating the cybersecurity incident investigative processes they follow.

The NCIP FORUM

First secure, hosted information sharing & collaboration environment for Local Law Enforcement and Cyber Investigative Firms

LIVE

31st March | 18.00

National Cybercrime Investigators Program
SUPPORT@NCIPFORUM.COM
1-402-915-1185

MISSION:
To enable cyber investigators and law enfrocement to achieve the "network effects" & "force multipliers" of investigative effectiveness and efficiency

Hosted through a Microsoft 365 Government G5 account

Supports CJIS and IRS 1075 standards and DISA Level 2 Security Requirements Guidelines, utilizing the intuitive Microsoft Teams Platform

01

Enables NCIP-Certified Investigators to connect, communicate, and engage with other NCIP-Certified Investigators

02

Securely discuss ideas, share updates and network; Create and edit documents, take notes, and share resources as LE-engaged groups

03

Send, view, prioritize, and manage messages; search for experts, conversations, and files; Join or create groups to stay informed and gather information & ideas on current cybercrime incidents

04

Users will be able to communicate in almost real-time through a web browser or mobile applications (Apple and Android devices)

05

The forum will take cyber security investigation communications and collaboration to the next level and will help the Local Law Enforcement community connect and engage nationwide on a secure platform

06

Access to the NCIP FORUM is limited to Law Enforcement agencies and NCIP-Certified Investigators.

Forum sponsored by National Cybercrime Investigators Program Information Sharing Environment (NCIP ISE) and the NSA "Cybersecurity and Crime Work Group"

The NCIP FORUM

First secure, hosted information sharing & collaboration environment for Local Law Enforcement and Cyber Investigative Firms

The much anticipated and much needed NCIP FORUM is ready to launch. The initial phase will consist of select group of (20) Users (Agencies or Firms) that will be able to access the NCIP FORUM for (90) days without being assessed the normal access fees. Each Agency or Firm will be allowed to select (3) Users from their organization to grant access to the NCIP Forum also without being assessed the normal access fees. These (20) agencies and their selected Users will explore the NCIP FORUM giving feedback on what works well, recommendations that could make it even more useful, and suggestions as to what additional features they would like to see added that might assist them

National Cybercrime Investigators Program
SUPPORT@NCIPFORUM.COM
1-402-915-1185

MISSION:
To enable cyber investigators and law enfrocement to achieve the "network effects" & "force multipliers" of investigative effectiveness and efficiency

Standard Fee Structure

NLEA AGENCY INITIAL SETUP FEE AND ANNUAL RENEWAL FEE $100 Setup Fee + $100 Annual Fee	=	**$200**
PRIVATE FIRM INITIAL SETUP AND ANNUAL RENEWAL FEE $600 Setup Fee + $1000 Annual Fee	=	**$1,600**
NLEA USER MONTHLY FEE Must be LE Agency Sponsored	=	**$25**
NCIF USER MONTHLY FEE Must be Firm Sponsored	=	**$120**
SECURE AREA RESTRICTED TO SHERIFFS AND CHIEFS OF POLICE Monthly Access Fee (Agency must be setup in Forum)	=	**$25**

If your Agency or Firm is receiving this notice you have been selected by NCIP as a highly regarded Agency or Firm that would be a great selection to be a NCIP FORUM Assessment participant. Listed below is the process and requirements to take advantage of this one time offer:

1. Confirm your acceptance of this one time offer as an NCIP FORUM Assessment User by contacting NCIP at Dennis Kelly; Secretary, NCIP; dkelly@ncip.tech; 504-251-0240.

2. Select your User/Users (3 max.) to represent your Agency/Firm in the NCIP FORUM.

3. Fill out the 'onboarding questionnaire' (provided upon acceptance of the offer) for your Agency and your selected Users.

4. You will be contacted by an NCIP Forum Operations Team member and receive your access instructions as well as how to provide your required feedback to the Team regarding your experience using the NCIP FORUM.

5. All Agencies or Firms, and associated users' fees (3 max.), will be waived for the (90) day assessment period. At the end of the (90) days, continued access to the NCIP FORUM will require submitting the applicable fees listed above.

Forum sponsored by National Cybercrime Investigators Program Information Sharing Environment
(NCIP ISE) and the NSA "Cybersecurity and Crime Work Group"

National Cybercrime Investigators Program (NCIP)

Sponsored by the e-Ponte Foundation

Law Enforcement Agency Introduction to NCIP & NCIP Certification

About NCIP: NCIP was developed by a National Sheriffs' Association (NSA) Work Group led by Sheriff David Goad, Allegany County, MD. It provides a pre-packaged set of services for Sheriffs and Chiefs, and the cyber incident investigation firms with which they choose to partner, aimed at enabling them to readily step up the cyber incident investigation services they provide for constituents. NCIP was launched at the instance of, and it is supported by, the National Sheriffs Association, see NSA Resolutions at https://www.ncip.tech/nsa-resolutions. It is also a supported activity of the Emergency Services Sector Coordinating Council, the single voice that DHS recognizes for the entire Emergency Services Sector, see https://www.sheriffs.org/content/emergency-service-sector-coordinating-council-esscc.

What NCIP Does: NCIP brings assistance to agencies in three key areas:

- **Cybercrime Victim Support**, through NCIP's partnership with Cybercrime Support Network, https://cybercrimesupport.org
- **Training,** especially low-cost or free training, for law enforcement personnel, namely
  - novice technical personnel interested in becoming experienced cyber experts;
  - experienced to expert technical personnel who are interested in increasing their technical knowledge and skills; and
  - non-technical personnel, like patrol personnel, who will never be technical cyber investigators but who can deal with the public on cyber complaints **(To be Implemented)**
- **Subscription-based Information sharing and collaboration services** by which an investigator at even the smallest and most remote local law enforcement agency can reach out to other cyber investigators and volunteer experts around the Nation for
  - technical collaboration and assistance on investigations (**NCIP FORUM**), as well as
  - Help Desk and Just-In-Time Emerging Threat Training (e.g., a new Ransomware threat) **(To be Implemented)**

NCIP believes that enabling local law enforcement info sharing and collaboration on cyber incident investigations, nationwide, will be an unprecedented accomplishment that can be a real game-changer for law enforcement.

FYI, NCIP does not charge for its services, though there are some charges for information sharing tools that must be sustained, which have been priced to law enforcement at the very low cost level necessary to sustain services, and some trainers have charges for some of the training.

To get started, NCIP needs agencies to document the personnel that they want to participate in NCIP as an NCIP-Certified Law Enforcement Investigator, by providing two documents:

- **NCIP Law Enforcement Agency (LEA) Application**—NCIP works with any accredited LEA that provides this documentation about the LEA;
- **NCIP Law Enforcement Investigator Application Form:** LEAs should provide one application for each Agency-affiliated person proposed by the LEA for NCIP-Certification as either
  - **NCIP-Certified Law Enforcement Investigator (NLEI)** (Agency-affiliated technical investigators) or
  - **NCIP-Certified Law Enforcement Investigation Manager (NLEIM)** (any Agency-affiliated person(s) that support or monitor Investigators' actions in the FORUM)

For Additional Info, Assistance and to Return these Forms: info@NCIP.tech

National Cybercrime Investigators Program

Sponsored by the e-Ponte Foundation

NCIP Law Enforcement Agency Application

The following information is provided by the below-named Applicant Law Enforcement Agency ("LEA") in connection with this its Application to be an NCIP-Certified Law Enforcement Agency.

Applicant LEA Name: ______________________________ ORI: _____________

State: ___ Description: ____

LEA Principal Office Address: ____

LEA Website: ____

Name of Agency Head: __________________ Title: ______________ Tel: ____________

Email:______________.

Name, Principal Secretary/Assistant to Agency Head: ___________________ Title: ___________ Tel: ______________ Email:______________

LEA Chief of Investigations: ______________________ Title: ___________ Tel: ____________

Email ______________ (Please attach Bio)

LEA's Cyber Investigation Services (please describe):___________________________________

____

LEA acknowledges that access to NCIP Systems is authorized only for authorized NCIP-Certified Law Enforcement and NCIP-Certified Cyber Investigators, and that, as an NCIP-Certified Law Enforcement Agency, the LEA and the NCIP-Certified Law Enforcement Investigators sponsored by it, will conform to all NCIP policies and procedures.

The above and attached information is correct, truthful and complete in all material respects.

______________________________________, Agency

BY:____________________________, Authorized Representative

TITLE: _________________________

DATE: _________________________

APPLICATION ACCEPTANCE: ______________, 20__

National Cybercrime Investigators Program

BY: _________________________________

Secretary

National Cybercrime Investigators Program

Sponsored by the e-Ponte Foundation

NCIP Law Enforcement Investigator Application Form

The following information is provided by the below-named Applicant in connection with his/her Application to be an NCIP-Recognized Law Enforcement Investigator.

Applicant NCIP Law Enforcement Investigator Information

Full Legal Name______________________________ Date of Birth ____/____/_____
Mo/Day/Yr

Any Also Known As_______________________

US Citizen: YES___NO___ Other Citizenship:_______ D/L No./State ________________/_____

Last (4) of SS # * ** __ __. __. __ (for LE verification of ID)**

Current Employer___________________________ Rank/Title_____________________________

Current Address____

Current Cyber and Cyber-related Certifications ____

Felony Convictions: YES______NO_______

Current BIO (attached)

Applicant for NCIP-Certified Law Enforcement Investigator ___ or NCIP-Certified Law Enforcement Investigation Administrator/Manager ___ (Limited Data Write Rights)

The above and attached information is correct, truthful and complete in all material respects.

_____________________________, Applicant

Printed Name____________________

Date: _____________________

Sponsoring Law Enforcement Agency

Based on due diligence prudent under the circumstances, and to the best of the undersigned Agency's knowledge, information and belief, the above and attached information is correct, truthful and complete in all material respects.

Comments or Exceptions, if any: ____

______________________________________, Law Enforcement Agency

BY:____________________________, Authorized Representative

RANK/TITLE: ____________________________

DATE: _________________________

www.NCIP.tech www.e-Ponte.tech info@NCIP.tech

National Cybercrime Investigators Program (NCIP)

Sponsored by the e-Ponte Foundation

Cyber Investigation Firm (CIF) Introduction to NCIP & NCIP Certification

About NCIP: NCIP was developed by a National Sheriffs' Association (NSA) Work Group led by Sheriff David Goad, Allegany County, MD. It provides a pre-packaged set of services for Sheriffs and Chiefs, and the cyber incident investigation firms with which they choose to partner, aimed at enabling them to readily step up the cyber incident investigation services they provide for constituents. NCIP was launched at the instance of, and it is supported by, the National Sheriffs Association, see NSA Resolutions at https://www.ncip.tech/nsa-resolutions. It is also a supported activity of the Emergency Services Sector Coordinating Council, the single voice that DHS recognizes for the entire Emergency Services Sector, see https://www.sheriffs.org/content/emergency-service-sector-coordinating-council-esscc.

What NCIP Does for CIFs: NCIP brings assistance to Law Enforcement Agencies and Cyber Investigation Firms (CIFs) in three key areas: Cybercrime Victim Support; Training, and Information Sharing & Collaboration. Law Enforcement Agencies have material unmet needs in all three of these areas, while Cyber Investigation Firms' most important need is in Information Sharing & Collaboration. Accordingly, NCIP's main value to CIFs is in this third area:

- **Subscription-based Information sharing and collaboration services:** services by which an investigator at even the smallest and most remote local law enforcement agency or the smallest Cyber Investigation Firm can reach out to other cyber investigators and volunteer experts around the Nation for
  - technical collaboration and assistance on investigations (**NCIP FORUM**), as well as
  - Help Desk and Just-In-Time Emerging Threat Training (e.g., a new Ransomware threat) **(To be Implemented)**

NCIP believes that enabling local law enforcement & CIF info sharing and collaboration on cyber incident investigations, nationwide, will be an unprecedented accomplishment that can be a real game-changer for law enforcement.

FYI, NCIP does not charge for its services, though there are some charges for information sharing tools that must be sustained, which have been priced to law enforcement at the very low cost level necessary to sustain services, and some trainers have charges for some of the training.

To get started, NCIP needs agencies to document the personnel that they want to participate in NCIP as an NCIP-Certified Law Enforcement Investigator, by providing two documents:

- **NCIP Cyber Investigation Firm (NCIF) Application**—NCIP works with any accredited LEA that provides this documentation about the CIF;
- **NCIP Cyber Investigator (NCI) Application Form:** CIFs should provide one application for each Agency-affiliated person proposed by the CIF for NCIP-Certification as either
  - **NCIP-Certified Cyber Investigation (NCI)** (CIF-affiliated technical investigators) or
  - **NCIP-Certified Cyber Investigation Manager (NCIM)** (any CIF-affiliated person(s) that support or monitor Investigators' actions in the FORUM)

For Additional Info, Assistance and to Return these Forms: info@NCIP.tech

National Cybercrime Investigators Program

Sponsored by the e-Ponte Foundation

NCIP Cyber Investigation Firm Application

The following information is provided by the below-named Applicant ("Firm") in connection with this its Application to be an NCIP-Certified Cyber Investigation Firm.

Applicant Cyber Investigation Firm: ______________________________. **EIN**: _______________

Legal Description: ___________________________ State: __ DBA: _________________________

Other Firm Status or Designations (e.g., Veteran, DBE or WOSB) _________________________

Firm Principal Business Office Address: ____

Firm CEO/Senior Officer: __________________ Tel: ____________ Email ______________

Lead Investigator: ______________________ Tel: ____________ Email ______________

Firm Website(s): ____

Firm's Cyber Investigation Services Description/Presentation (attached)

Firm Lead Investigator Bio (attached)

Firm acknowledges that access to NCIP Systems is authorized only for authorized NCIP Law Enforcement Investigators and NCIP-Certified Cyber Investigators, and that, as an NCIP-Certified Cyber Investigation Firm, the Firm and the NCIP-Certified Cyber Investigators sponsored by it, will conform to all NCIP policies and procedures.

The above and attached information is correct, truthful and complete in all material respects.

_______________________________________, Firm

BY:____________________________, Authorized Representative

TITLE: _________________________

DATE: _________________________

APPLICATION ACCEPTANCE: ______________, 20__
National Cybercrime Investigators Program

BY: __________________________________
Secretary

National Cybercrime Investigators Program

Sponsored by the e-Ponte Foundation

NCIP Cyber Investigator Application

The following information is provided by the below-named Applicant in connection with his/her Application to be an NCIP-Certified Cyber Investigator.

Applicant NCIP Cyber Investigator Information

Full Legal Name______________________________ Date of Birth ____/____/_____
Mo/Day/Yr

Any Also Known As___________________________

US Citizen: YES___NO___ Other Citizenship:_______ D/L No./State ________________/____

Last (4) of SS # * ** __ __. __. __ (for LE verification of ID)**

Current Address____

Current Employer/Job Title____

Current Cyber and Cyber-related Certifications ________________________________

Felony Convictions: YES______NO_______

Current BIO (attached)

Applicant for NCIP-Certified Cyber Investigator ___ or NCIP-Certified Cyber Investigation Manager ___ (Limited Data Write Rights)

The above and attached information is correct, truthful and complete in all material respects.

_____________________________, Applicant NCIP Cyber Investigator

Printed____________________

Date: ____________________

Sponsoring Cyber Investigation Firm

Based on due diligence prudent under the circumstances, and to the best of the undersigned Firm's knowledge, information and belief, the above and attached information is correct, truthful and complete in all material respects.

Comments or Exceptions, if any: ____

______________________________________, Sponsoring Cyber Investigation Firm

BY:____________________________, Authorized Representative

TITLE: _________________________

DATE: _________________________

TAB C

C. ABOUT CYBER ENABLED CRIME INVESTIGATIONS

C.1 ABOUT THE SCIO APP

C.2 NCIP NON-TECHNICAL TRAINING FOR INVESTIGATORS OF CYBER ENABLED CRIME

ABOUT CYBER-ENABLED CRIME INVESTIGATIONS

In many ways, the direction of NCIP's Cyber Investigation Program reflects the lessons learned, and path blazed by, NYPD in its efforts to fulfill its law enforcement charter and organizational mandate to meaningfully respond to constituent complaints of "Cybercrimes".

That is, NYPD launched its NYPD Cyber Investigative Standards Pilot Program, and, in the process, found that the term "Cybercrime" is overbroad and confusing, from an investigative perspective. NYPD also developed the understanding of the "cybercrime" problem from an investigative perspective that many "cyber" cases could be investigated and cleared using traditional policing methods and processes, and without any meaningful technical "cyber" knowledge, while other cases require deep technical "cyber" knowledge in order to be cleared. Concluding that the term "Cybercrime" should be replaced with less confusing terminology, NYPD coined two new terms for these two types of cases: "Cyber Enabled Crimes" and "Cyber Native Crimes".

Here's what these two terms refer to:

- **Cyber Enabled Crimes** are traditional crimes abetted by cyber tools (e.g., **fraud, scams, larceny, grand larceny, and extortion**); or facilitated by use of cyber tools, like coordination or planning of traditional crimes using digital devices like phones or computers. Cyber Enabled cases, then, can be investigated and cleared using traditional policing methods and processes.
- **Cyber Native Crimes**, on the other hand, are crimes (like **cryptocurrency hacking, network intrusion, election tampering** or **data theft**) that could not be committed outside the digital domain. Cyber Native cases require deep technical "cyber" knowledge in order to be cleared.

NCIP's Cyber Enabled Investigations Program, discussed in this section, is based on the "lessons learned" by NYPD in developing its understanding of Cyber Enabled Crimes, and is executed using the SCIO App and SCIO App Training provided to law enforcement agencies at no charge.

The SCIO App is the key component of NCIP's Cyber Enabled Investigations Program. It was developed by Nick Selby, former NYPD Director of Cyber Intelligence and Investigations, and Raven Zachary, and tested in the field in support of the NYPD Cyber Investigative Standards Pilot Program. Through a partnership with Mr. Selby, NCIP is making the SCIO App available to local law enforcement agencies at no charge.

National Cybercrime Investigators Program

FOR LAW ENFORCEMENT USE ONLY/LAW ENFORCEMENT SENSITIVE

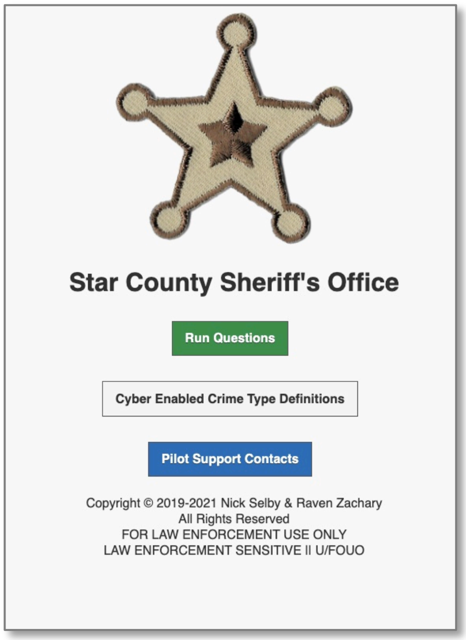
ABOUT THE SCIO APP & SCIO APP TRAINING
For Cybercrime Investigations by Any Law Enforcement Agency In The Nation

The SCIO APP (the "App"), Developed for NYPD, Now Available to Any Agency, at No Charge

The SCIO App, with associated training, was originally developed for NYPD by NYPD's Nick Selby and Raven Zachary as a tool for non-technical NYPD Patrol Officers to investigate traditional crimes abetted by cyber tools (e.g., **fraud, scams, larceny, grand larceny** and **extortion**) (also referred to as "**Cyber Enabled**" **crimes**).

Then, in the **NYPD Cyber Investigative Standards Pilot Program**, **NYPD leadership trained 700+ non-technical NYPD Patrol officers** who field tested and successfully used the App to investigate complaints of Cyber Enabled crimes. NYPD leadership has concluded that the SCIO App provides the additional tools and knowledge that non-technical officers need to investigate and clear Cyber Enabled crimes, and NYPD now uses the App as a tool for officers to investigate and share information about Cyber Enabled crimes.

Now, NYPD and Mr. Selby are providing the SCIO App for NCIP to provide the App and App training to **any accredited law enforcement agency in the Nation, all at no charge to agencies.**


Star County Sheriff's Office
Run Questions
Cyber Enabled Crime Type Definitions
Pilot Support Contacts

Copyright © 2019-2021 Nick Selby & Raven Zachary
All Rights Reserved
FOR LAW ENFORCEMENT USE ONLY
LAW ENFORCEMENT SENSITIVE II U/FOUO

The SCIO App and SCIO App Training

Training non-technical investigators to use the SCIO App takes about 15 minutes and is typically conducted by non-technical agency leaders at Roll Call using NYPD-developed and NCIP-supplied training material.

The SCIO App enables non-technical investigators to ask a series of questions about each incident, to collect and share data about the incident, and to handle the incident as they would in any other traditional crime investigation.

App Configuration & Administering App-collected Data

Requesting agencies will be licensed to use the SCIO App, **without charge.** Each agency personalizes its licensed copy of the App, runs its copy of the App on its server and manages use of the App by its officers, and the data they collect using the App. **Each agency that opts in to share their App-collected data through NCIP will have access to traditional crime data collected by NCIP from other NCIP-participating agencies,** under operational policies and procedures established by NCIP's Staff and approved by NCIP's Executive Committee.

Having An Experienced Voice At Hand During the Migration to the "New Normal"

NYPD found it useful to establish a "Detectives Help Desk" to serve as an experienced voice and "out of the box" resource for non-technical investigators as they learn how to think about Cyber Enabled crimes, and how to use the SCIO App to investigate traditional crimes committed using cyber tools. Agencies using the App should consider doing the same thing.

For Additional Information
Sheriff David Goad, NCIP CEO: 301-268-2901, dgoad@NCIP.tech
Dennis Kelly, Esq., NCIP General Counsel: 504-251-0240, dkelly@NCIP.tech

info@ncip.tech **504-717-4872** **©e-Ponte Foundation, 2021**
www.NCIP.tech **www.e-Ponte.tech**

NCIP Non-Technical Training for Investigators of Cyber Enabled Crime

Enabling Engagement By
Local Law Enforcement Agencies
Nationwide, Based on Lessons Learned by NYPD

June 2021

NCIP

- Was launched by the National Sheriffs' Association, and is supported by NSA Resolutions
- Is a Reporting Program of the Emergency Services Sector Coordinating Council (ESSCC)
- Is supported by The e-Ponte Foundation

NCIP's Cyber Investigative Programs are based on Lessons Learned from NYPD's Cyber Investigative Standards Pilot Program, and are being implemented with assistance of NYPD Deputy Chief John Hart, Nick Selby, former NYPD Director of Cyber Intelligence and Investigations, and other NYPD Executives

Defining Cyber Crime

There are two broad categories of Cyber Crime:

- **Cyber Enabled Crimes:** Traditional crime abetted by cyber tools (e.g., **fraud, larceny and grand larceny**); or facilitated by use of cyber, like coordination or planning of traditional crimes using digital devices like phones or computers. This CEIP Program provides tools for local law enforcement to respond to public complaints of Cyber Enabled crimes.
- **Cyber Native Crimes:** Crimes (like **cryptocurrency hacking, network intrusion, election tampering or data theft**) that could not be committed outside the digital domain. We’re talking criminal and nation-state hackers.

Responding to Cyber Enabled and Cyber Native Crime Complaints

- NCIP’s Cyber Enabled Investigative Program (CEIP) enables non-technical law enforcement officers to respond to public complaints of Cyber Enabled crimes.
- NCIP’s CEIP Program does not address Cyber Native crimes, which require more specialized investigative tools and expertise.
- NCIP’s separate Cyber Native Investigative Program (CNIP) provides tools for local law enforcement agencies to respond to public complaints of Cyber Native crimes.

How Many of your Constituents are Victims of Cybercrime? How big is its Financial Impact?

- You cannot manage what you cannot measure.
- NYPD was astonished at how much Cyber Enabled Crime victimized New Yorkers.
- A Key Purpose of the NCIP CEIP Program is to help grow the collection and reporting of Cyber Enabled Crimes across the Nation at the agency level and nationally, so Law Enforcement Leaders and Policy-makers have some sense of the level of Cyber Enabled Crime that is taking place.

NYPD Learned that Cyber Enabled Crime Victimized New Yorkers, In a Very Big Way

2019 CYBER ENABLED CRIMES

NYC	PROJECTED # SCAM VICTIMS	PROJECTED FINANCIAL IMPACT
CITYWIDE (Pops: 18.8MM)	15,340	$224 million
QUEENS (Pops: 2.2MM)	3,410	$37.1 million
QUEENS SOUTH (Pops: 974M)	970	$10.6 million

PROJECTED AVG IMPACT PER VICTIM CITYWIDE: $14,623

At $14,263 Per Victim, What Is Cyber Enabled Crime’s Impact in your Jurisdiction?

- Assume $14,263/Victim Impact (NYC rate)
- Assume 0.1% of the Population are Victims, annually.

Victim Rate	Pops.	# Victims	Annual Financial Impact
0.1%	500,000	500	$7,130,000
0.1%	100,000	100	$1,430,000
0.1%	50,000	50	$713,000

TOP THREE SCAMS BY DOLLAR AMOUNT (NYC, CITYWIDE, 2019)

- Fraud Email/Impersonation: $125 million
- Call Fraud (Government): $52.8 million
- Account Takeover: $19.2 million

Types of Cyber Enabled Scams

-Fraud Email/Impersonation

-Call Fraud (Government)

-Call Fraud (Other)

-New Fraud: Uber Driver Scam

-Online Extortion (reputational)

-Extortion(Physical)

-SIM-Swap

-Scam Webpage or Financial Transaction

-Malware/Redirect/SEO Scam

-Account Takeover

Taking Cyber Enabled Crime Complaints

- A typical Complainant/Victim reports a crime that involves a cyber element like a scam phone call or email, or use of a gift card or Bitcoin.

- The suspects will not be charged with “hacking” or computer crime. They will be charged with, for example, Grand Larceny.

We Can Get Them

- You don’t need to know “cyber” any more than you know fingerprints and DNA - just know that it is important to get and record the details.

- Just like any other job: we need the **what, when, where**, and **how**?

- **“Who”** and **“Why”** are detectives’ problem.

When Writing Your Report

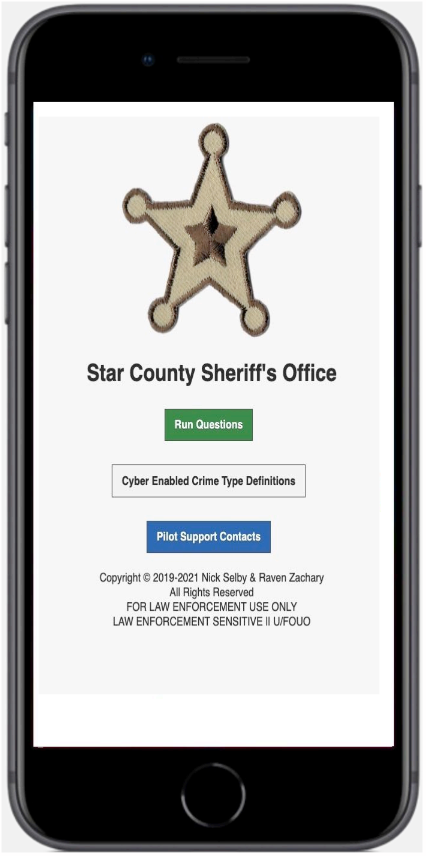
- When writing your Report, please put this code in the narrative:

CEIP-1

- and please select “Cyber Enabled Crime - YES” from the dropdown box in the App.

SCIO Application

From your work smartphone,
open the browser and
enter this URL:
https://NCIP.tech/SCIO/

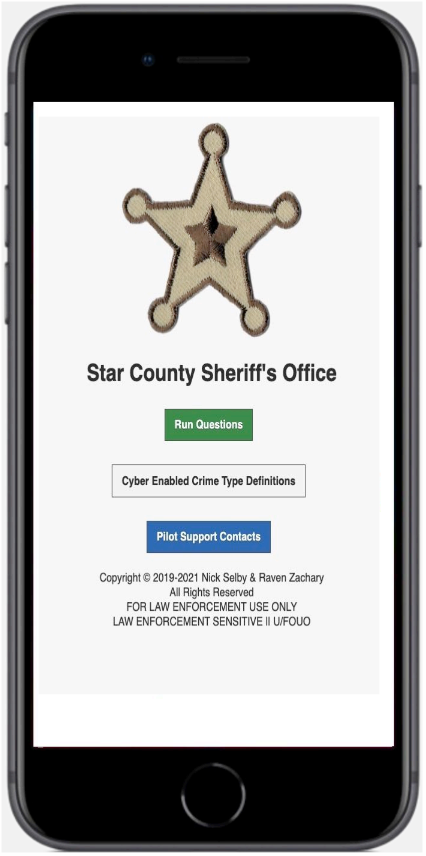


Star County Sheriff's Office

Copyright © 2019-2021 Nick Selby & Raven Zachary
All Rights Reserved
FOR LAW ENFORCEMENT USE ONLY
LAW ENFORCEMENT SENSITIVE II U/FOUO

Ask the questions and enter into your Report

- Select “Run Questions”
- Select the following questions on the app:
  - The kind of scam.
  - The method used to contact the victim.
  - The method of payment requested.
  - How the payment was made.
- The app gives you the questions to ask the Complainant/Victim.
  Ask the questions and enter the answers in your Report Narrative


Star County Sheriff's Office
Run Questions
Cyber Enabled Crime Type Definitions
Pilot Support Contacts

Copyright © 2019-2021 Nick Selby & Raven Zachary
All Rights Reserved
FOR LAW ENFORCEMENT USE ONLY
LAW ENFORCEMENT SENSITIVE || U/FOUO

QUESTIONS?

Support & Contacts

We are available from 8:00 am-6:00 pm, seven days a week. We will answer or, if you leave a message, call you back shortly.

CEIP Support Contacts: Info@NCIP.tech or 504-717-4872

Main NCIP email: Info@NCIP.tech

Sheriff David Goad, NCIP Chair: dgoad@NCIP.tech

Dennis Kelly, Esq., NCIP Secretary & General Counsel: dkelly@NCIP.tech

Acknowledgments

- The NCIP Cyber Enabled Investigations Program ("CEIP") is based on the Lessons Learned by NYPD during the highly-successful NYPD Cyber Investigative Standards Pilot Program ("Pilot Program").
- The CEIP's purpose is to provide to law enforcement agencies across the Nation, at no charge, training materials and tools to enable their Patrol and other Non-Technical personnel to field complaints from the public about cyber-enabled and other crimes committed against them.
- The CEIP's slides draw heavily from NYPD's training slides developed for the NYPD Pilot Program. NCIP wishes to thank NYPD, and Nick Selby, former NYPD Director of Cyber Intelligence and Investigations, for their significant contribution, through the NYPD Pilot Program, to 21st Century law enforcement.
- For more information, see https://www.youtube.com/watch?v=-_F8QdyKkeQ

TAB D

National Cybercrime Investigators Program

ABOUT CYBER NATIVE CRIME INVESTIGATIONS

Building on the lessons learned and path blazed by NYPD in its efforts to fulfill its law enforcement charter and organizational mandate to meaningfully respond to constituent complaints of "Cybercrimes", NCIP has embraced the two terms coined by NYPD to less confusingly, and, from an investigative perspective, more accurately describe two different types of cyber-involved crime.

Here's a thumbnail sketch of those two types of cyber-involved crime:

- **Cyber Enabled Crimes** are traditional crimes abetted by cyber tools (e.g., **fraud, scams, larceny, grand larceny, and extortion**); or facilitated by use of cyber tools, like coordination or planning of traditional crimes using digital devices like phones or computers. Cyber Enabled cases, then, can be investigated and cleared using traditional policing methods and processes, with little or no technical "cyber" expertise.
- **Cyber Native Crimes**, on the other hand, are crimes (like **cryptocurrency hacking, network intrusion, election tampering** or **data theft**) that cannot be committed outside the digital domain. Cyber Native cases typically require significantly deeper technical "cyber" knowledge in order to be cleared.

NCIP's Cyber Enabled Investigations Program is executed using the SCIO App and SCIO App Training provided to law enforcement agencies at no charge.

NCIP's Cyber Native Investigations Program, on the other hand, is executed using two different sets of tools, both of which are provided by NCIP, also at no charge to law enforcement agencies. Those two sets of tools are:

- **NCIP-Standard Cyber Native Playbooks;** and
- **NCIP Incident Data Reports.**

A key driver behind NCIP's adoption of these two standardized sets of tools for NCIP's Cyber Native Investigations Program is the utility and value to the law enforcement enterprise of standardized investigative processes being widely used by many of the Nation's some 17,000 local law enforcement agencies. That is, material efficiency and effectiveness gains can be expected from widespread law enforcement agencies' use of

- **A common set of Playbooks,** because that will allow training to be delivered in reference to a common investigative platform, and it will also allow a common base for Cyber Native Help Desk operations to more efficiently assist investigators of Cyber Native incidents, and also to more effectively use the Cyber Native Help Desk function to grow investigators' expertise; and
- **A common set of Incident Data Reports,** because that will provide a common basis for information sharing by investigators all across the Nation.

National Cybercrime Investigators Program

ABOUT NCIP INCIDENT DATA REPORTS

NCIP has developed a set of NCIP Incident Data Reports as standard tools to be used in support of NCIP-Standard Cyber Native Playbooks in conducting Cyber Native Crime Investigations.

NCIP-Standard Cyber Native Playbooks provide a standard set of operational procedures to be used in planning and conducting a cybersecurity vulnerability and incident response activity: each conforms to authoritative guidance in NIST SPECIAL PUBLICATION 800-61, REV 2, "Computer Security Incident Handling Guide".

Used in concert with these Playbooks, NCIP Incident Data Reports are used by Entry Level (or higher) Cyber Investigators during the Preliminary Investigation Phase of a Cyber Native Complaint to collect data about the incident, to share investigative information with other law enforcement agencies and/or to request for technical investigative assistance from the NCIP Cyber Forensics Laboratory (CFL), your FBI Field Office Cyber Task Force, a Regional Cyber Task Force, or another technically proficient cyber investigation resource.

The NCIP INCIDENT DATA REPORT DOCUMENTS consist of four NCIP Cyber Forensic Laboratory (CFL) Data Report Forms, as follows:

1. **CFL FORM 1: Forensic Incident Data Report**—used by technically proficient investigators to document information collected during the Preliminary Investigation regarding any type of Cyber Native Incident, and to place Forensic Incident Service Orders with the NCIP Cyber Forensics Laboratory (CFL), or other technically proficient cyber investigation resource.
2. **CFL FORM 2: Intrusion Incident Data Report**—used to document additional information collected during the Preliminary Investigation regarding Intrusion Incidents, and to place Intrusion Incident Service Orders with the NCIP Cyber Forensics Laboratory (CFL), or other technically proficient cyber investigation resource.
3. **CFL FORM 3: Media Recovery Data Report**—used to document additional information collected during the Preliminary Investigation regarding media recovery assistance needed, and to place Media Recovery Service Orders with the NCIP Cyber Forensics Laboratory (CFL), or other technically proficient cyber investigation resource.
4. **CFL FORM 4: Prosecution Support Data Report**—used by Detectives to place Prosecution Support Service Orders with the NCIP Cyber Forensics Laboratory (CFL), or other technically proficient cyber investigation resource.

These Report forms cover almost every aspect of their subject matter, and are intended to be completed to the extent useful to the Cyber Investigators working the case (i.e., it is not necessary to complete every blank).

In addition, the NCIP INCIDENT DATA REPORT DOCUMENTS include the CFL Service Order and CFL Standard Terms of Service, for use when CFL's support is requested.

National Cybercrime Investigators Program

CFL Form 1: Forensic Incident Data Report

This Report is used to compile Agency data on Forensic Incidents for further investigation.

AGENCY INFORMATION

1.Agency	**2.ORI**	**3.Date**	
4.Agency Case #	**5.Case Type**		
6.Case Agent Name	**7.Agent's Work #**	**8.Agent's Cell #**	
9.Agent's Email	**10.Agent's Badge #**		
11.Agent's Physical Address			
12.Supervisor's Name	**13.Supervisor's Work #**	**14.Supervisor's Cell #**	
15.Supervisor's Email	**16.Supervisor's Badge #**		
17.Case Sensitivity	**18.Alternate Agent**	**19.Alt. Agent's Best Tel #**	
20.Evidence Return Address	**21.Report Return Address**		
22.Court Name/Division	**23.Next Known Proceeding Date**	**24.Type of Proceeding**	
25.Prosecutor POC	**26.Work Phone**	**27.Title**	
28.ProsecutorAddress	**29.Prosecutor Email**		
30.Subject's Name	**31.Subject's DOB**		
32.Deceased/Victim Name	**33.Victim Is a Minor** □	**34. Victim's DOB**	**35.Relevant Dates**
36.Needed Service Type	**37.Associated Case(s)**		
38.Is new evidence being provided today? □	**39.Has any other person accessed the evidence? (provide details)**		
40.Additional Comments			

41.Check all items attached to this document:

__ Confession/statement from accused
__ Witness Statement.
__ Charge Sheets
__ Report for related Online Investigation

__ Photo of victim
__ Photo of subject
__ Defense expert Info
__ Prior forensic analysis

42.A. Needed Services. Provide an overview of needed services. Explain all checked boxes in item 41. Provide any key information pertinent to the investigation such as timeframes, email addresses, phone numbers, log-in details, passwords, etc. Attach additional sheets if needed.

42.B. Details of Needed Services. Search Timeframe: ___________________________________

Search Type: _______________________ Evidence Type: ___________________________________

Search/analyze the evidence for the following checked artifacts:

CHAT
___ All
___AiM
___ Google
___ iMessage
___ Lync
___ Skype
___ Yahoo Messenger
___ Other: ________

EMAIL
___ All
___ Gmail
___ Outlook
___ Hotmail
___ Yahoo
___ Other: ________

___ PASSWORDS

CLOUD SERVICE
___ All
___ Carbonite
___ Dropbox
___ OneDrive
___ Google Drive
___ iCloud
___ Other: ________

ARCHIVE FILES
___ All
___ RAR
___ Zip
___ Other: ________

MEDIA
___ All
___ Videos
___ Pictures
___ Other: ________

DOCUMENTS
___ All
___ Excel
___ PowerPoint
___ Word
___ Text
___ PDF
___ Other: _______

INTERNET HISTORY
___ All
___ Internet Explorer
___ Firefox
___ Chrome
___ Safari
___ Opera
___ Other: ________

SOCIAL MEDIA
___ All
___ Facebook
___ Instagram
___ MySpace
___ Twitter
___ Snapchat
___ Skype
___ Other: ______

PEER-TO-PEER
___ All
___ Limewire
___ Torren
___ eMule
___ Ares
___ Other: ________

___ ENCRYPTION

OS ARTIFACTS
___ All
___ Programs
___ Jumplist
___ LNK Files
___ Users
___ Keyword Searches
___ USB Devices
___ Prefetch Files
___ Logon Banner
___ Event Logs
___ Other: _____

ANTI-FORENSIC APPS
___ All
___ CCleaner
___ BCWipe
___ Other: ________

43A. **Priority Investigative Needs**: Check all items that apply to these needed services:

___ Pending key interviews
___ Pre-trial confinement (PTC)
___ Court deadlines

___ Evidence seized on consent (SUBJECT)
___ High-profile investigation
___ Password(s) identification

___ SUBJECT identification
___ Victim identification
___ Other: _______________

44.B. Additional Information: Explain in detail any additional information of which the CFL Examiner should be made aware. Attach additional sheets if needed.

45. **Note: Case Background:**

- Provide any background information relevant to this case.
- Provide allegations against the SUBJECT and who provided them.
- Provide Investigative Summary.

Note: Please attach additional sheets if needed.

46. Evidence List:

Enter information regarding media available for examination below. Attach additional sheets if needed.

Evidence List

Doc. #	Investigative Priority	Description	Sensitivity Indicator

Instructions Regarding Destruction & Destructive/Non-Destructive Methods

As of the date of this Form (please check):

□ Agency agrees to paragraph 7 of NCIP CFL Terms of Service regarding non-destructive/destructive methods of mobile devices.

□ Agency approval of destructive methods is awaiting legal review: further communication will be forthcoming.

*****IMPORTANT INFORMATION*****

DO NOT ATTACH BIOHAZARDOUS MATERIAL

National Cybercrime Investigators Program

CFL Form 1: Forensic Incident Data Report

This Forensic Incident Data Report should be as complete as possible. If the information on this form is not complete or accurate, any response may be delayed. If applicable, include the following items: Evidence Custody Documents, Consent to Search, Search Authority, and Law Enforcement Agency Sticker or Tag (for Agency-owned computers, smartphones, etc.).

Evidence can be delivered to CFL by registered mail, FedEx, or UPS, or agent drop off at NCIP CFL.

This Forensic Incident Data Report completed and signed, as follows.

DATE: ________________, 202__

________________________, Agency

____
Authorized Agent

ABOUT NCIP-STANDARD CYBER NATIVE PLAYBOOKS

A Playbook is a standard set of operational procedures to be used in planning and conducting a cybersecurity vulnerability and incident response activity.

In order to provide a standard approach to investigating Cyber Native Crime Complaints, and to facilitate Help Desk Operations in acting as a resource for law enforcement investigators, NCIP recommends that NCIP-participating agencies conduct Cyber Native Investigations using a common set of cybersecurity industry Playbooks provided to investigators at no charge here.

A different Playbook is provided for each of the following types of Cyber Native Incidents:

- Malware Outbreak Incident
- Unauthorized Access Incident
- Data Theft Incident
- Improper Computer Usage Incident
- Elevation of Privilege Incident
- Distributed Denial of Service (DDoS) Incident
- Phishing Incident
- Virus Outbreak Incident
- Root Access Incident

This set of Playbooks does not completely cover every type of Cyber Native incident, and other Playbooks will be developed over time. Over time, NCIP also anticipates refining these Playboks based on law enforcement agency feedback, and automating Playbooks for efficiency and effectiveness gains, including automation of investigation tasks and information sharing.

As a tool for carrying out Playbook-based Cyber Native Investigations, NCIP also provides a set of Incident Data Reports, that may be used to complete a Preliminary Investigation of any Cyber Native Incident. These Incident Data Reports may be made available to the NCIP Cyber Forensic Laboratory, your FBI Field Office Cyber Task Force, a Regional Cyber Task Force, or to another technically proficient cyber investigation resource. See "ABOUT NCIP INCIDENT DATA REPORTS".

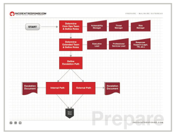
NCIP recognizes that, given the current state of implemented cybersecurity defenses, and the resource constraints under which local law enforcement operates, many Cyber Native Investigations will reach the status of "All investigative leads are extinguished", and left in "unsolved inventory". Inability to clear investigations is a cost of doing an investigative business, but sharing with others the investigative information that has been collected mitigates this cost by benefiting other investigations. See "ABOUT THE NCIP FORUM INFORMATION SHARING ENVIRONMENT".

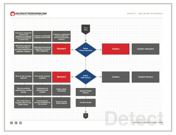
INCIDENTRESPONSE.COM
ONLINE INCIDENT RESPONSE COMMUNITY

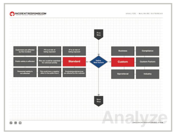
Automate Response

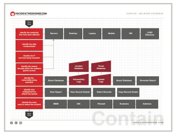
Congratulations on selecting **IncidentResponse.com** to retrieve your custom incident response playbook guide. This guide has been created especially for you for use in within your security response team. We hope you find it valuable and ask that you share it with the rest of your organization so you can collectively be successful in managing incidents and reducing risk throughout the business.

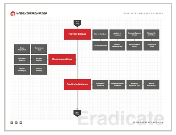
Your playbook overview - "Malware Outbreak"

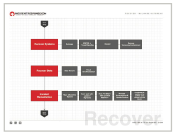


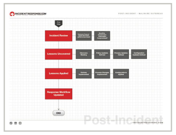












Incident Response: A Top Priority in Security Management Programs

In the April 2014, U.S. Government Accountability Office reported (GAO-14-354) it's noted that "major federal agencies did not consistently demonstrate that they are effectively responding to cyber incidents (a security breach of a computerized system and information)." The GAO projects that these agencies did not completely document actions taken in response to detected incidents. While the agencies identified the scope of an incident, they frequently did not demonstrate that they had determined the impact of an incident, nor did they consistently demonstrate how they had handled other key activities, such as whether preventive actions to prevent the reoccurrence of an incident were taken. The GAO notes, "without complete policies, plans, and procedures, along with appropriate oversight of response activities, agencies face reduced assurance that they can effectively respond to cyber incidents." [3]

Did you know?

In **2014**, incidents **increased by 78% since 2013.**[1]

1,023,108,627 records were breached in **2014**.[1]

54% of the breaches consisted of **Identity Theft**.[1]

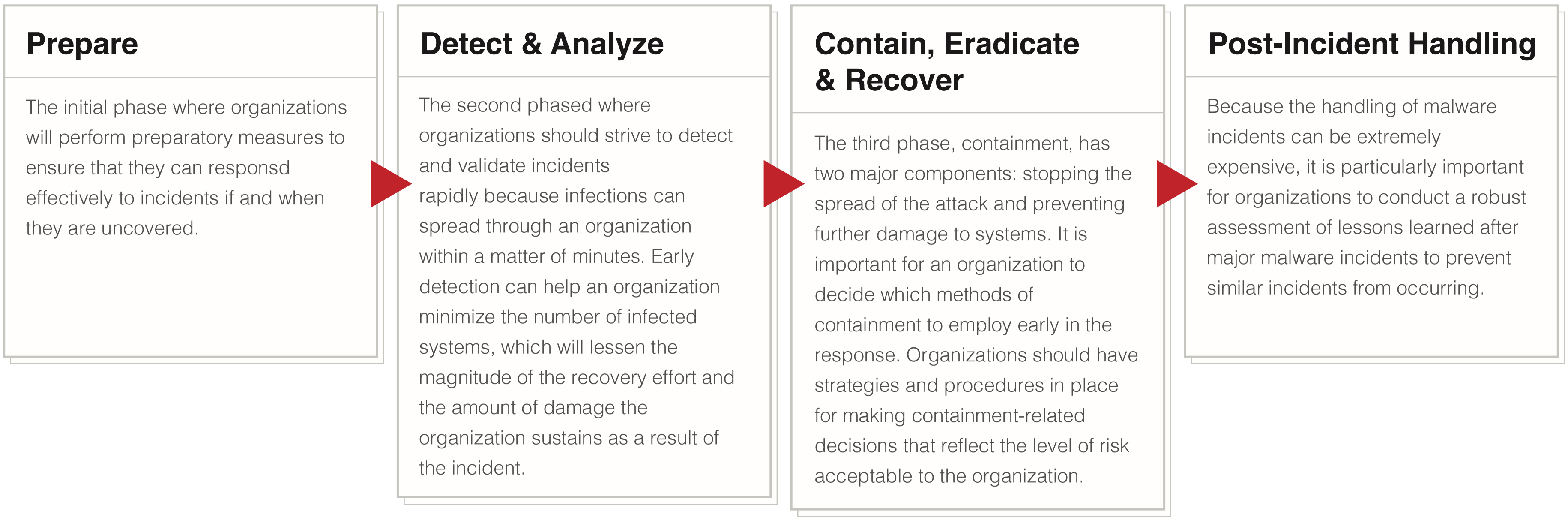
$3.5 million is the **average cost of a breach** for a company.[2]

Companies experience an average of **10 unauthorized access incidents per month.**[2]

Malicious insiders and **criminal attacks** are the top causes for breaches.[2]

1. ***Source**: Gemalto - Breach Level Index*
2. ***Source**: Ponemon 2014 Cost of a Data Breach*
3. ***Source:** GAO-14-354, p.2*

What is an incident response playbook? According to NIST Special Publication 800-61, an incident response process contains four main phases: preparation, detection and analysis, containment/eradication/reocvery, and post-incident activity. Descriptions for each are included below:



Prepare

The initial phase where organizations will perform preparatory measures to ensure that they can responsd effectively to incidents if and when they are uncovered.

Detect & Analyze

The second phased where organizations should strive to detect and validate incidents rapidly because infections can spread through an organization within a matter of minutes. Early detection can help an organization minimize the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organization sustains as a result of the incident.

Contain, Eradicate & Recover

The third phase, containment, has two major components: stopping the spread of the attack and preventing further damage to systems. It is important for an organization to decide which methods of containment to employ early in the response. Organizations should have strategies and procedures in place for making containment-related decisions that reflect the level of risk acceptable to the organization.

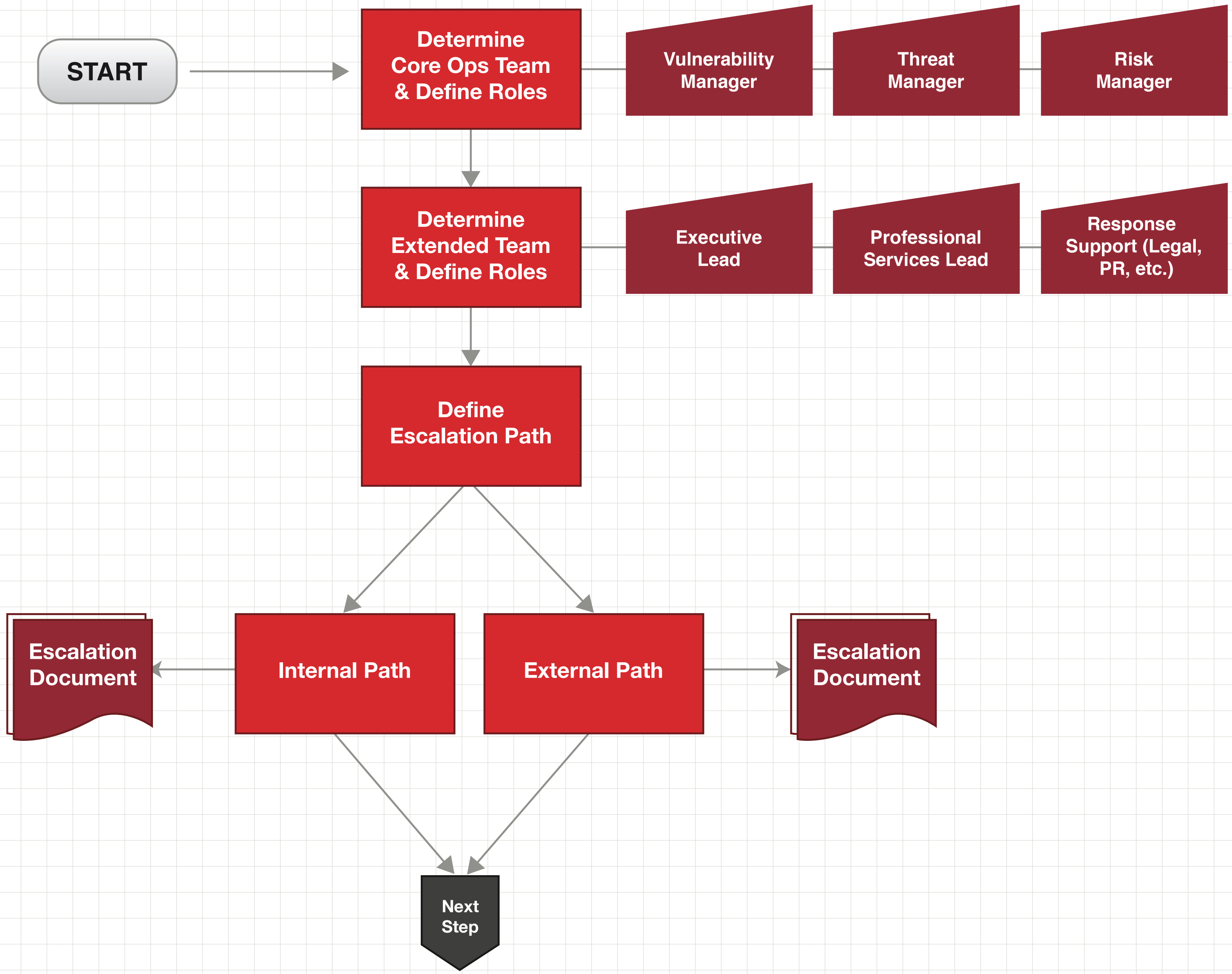
Post-Incident Handling

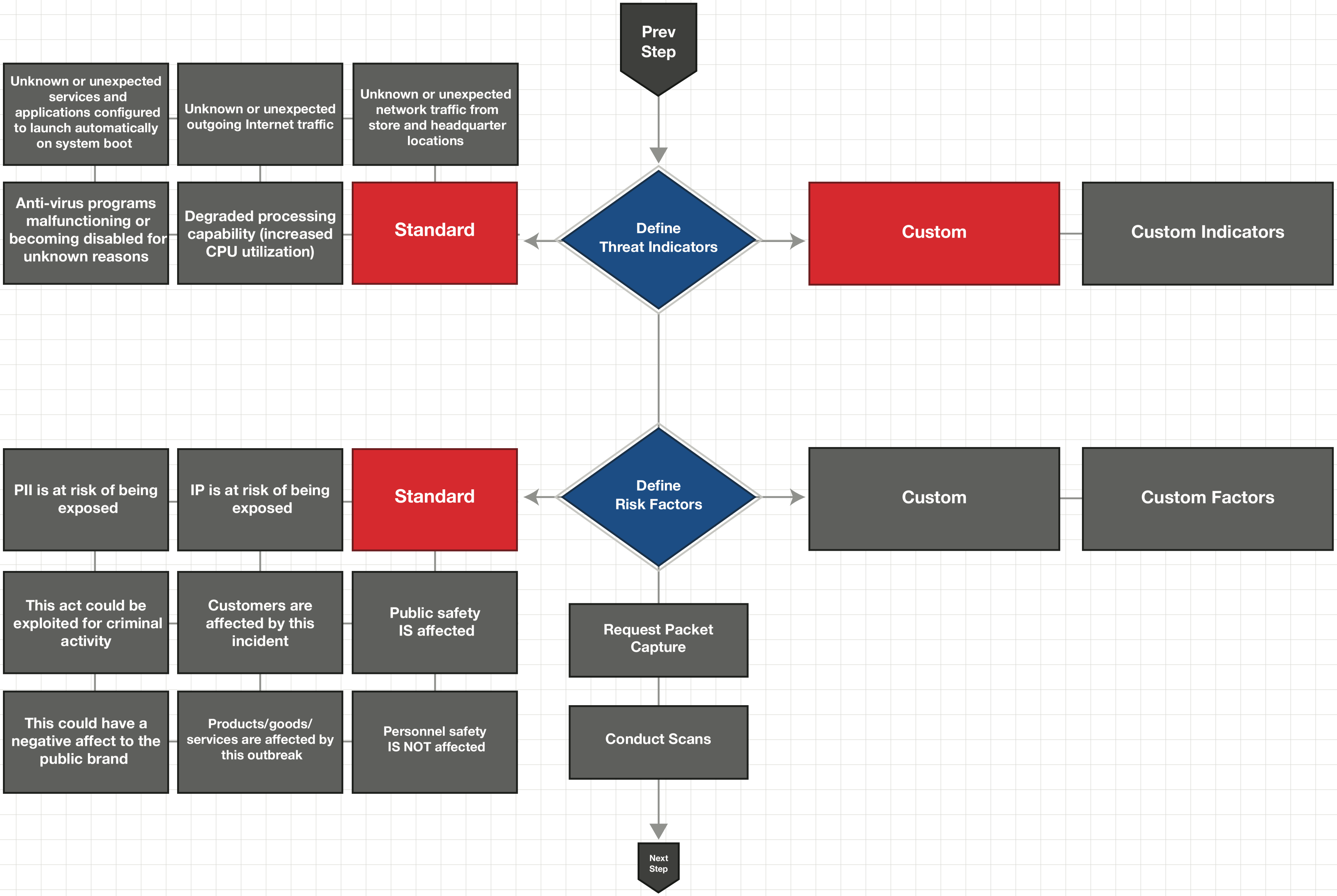
Because the handling of malware incidents can be extremely expensive, it is particularly important for organizations to conduct a robust assessment of lessons learned after major malware incidents to prevent similar incidents from occurring.

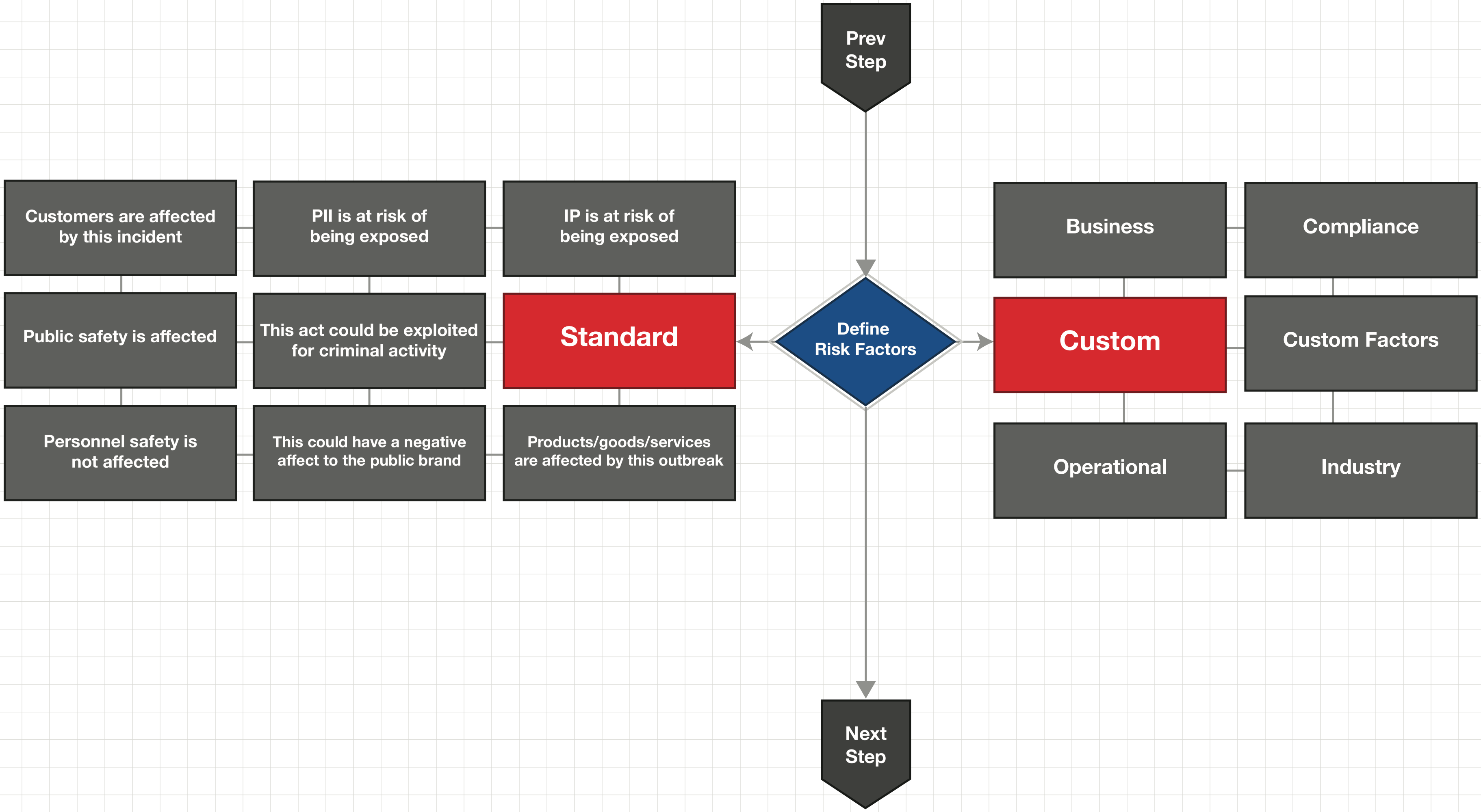
Malware Outbreak

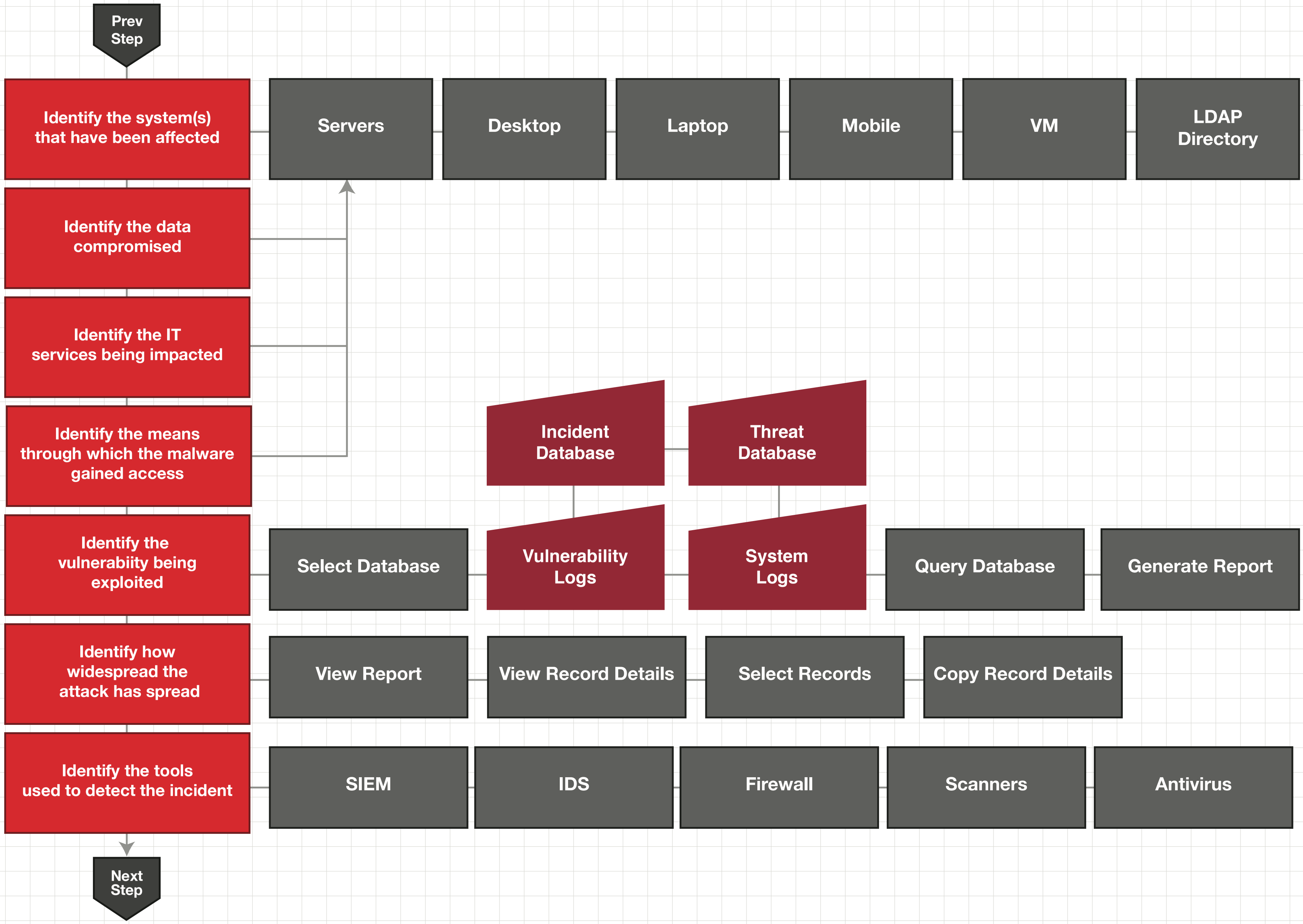
You've selected the "**Malware Outbreak**" playbook. On the pages that follow, you will find your incident response playbook details broken down by the NIST incident handling categories.

To view your playbook online, visit **https://incidentresponse.com/playbooks/malware-outbreak**


START
Determine
Core Ops Team
& Define Roles
Vulnerability
Manager
Threat
Manager
Risk
Manager
Determine
Extended Team
& Define Roles
Executive
Lead
Professional
Services Lead
Response
Support (Legal,
PR, etc.)
Define
Escalation Path
Escalation
Document
Internal Path
External Path
Escalation
Document
Next
Step


Prev Step
Define Threat Indicators
Standard
Unknown or unexpected services and applications configured to launch automatically on system boot
Unknown or unexpected outgoing Internet traffic
Unknown or unexpected network traffic from store and headquarter locations
Anti-virus programs malfunctioning or becoming disabled for unknown reasons
Degraded processing capability (increased CPU utilization)
Custom
Custom Indicators
Define Risk Factors
Standard
PII is at risk of being exposed
IP is at risk of being exposed
This act could be exploited for criminal activity
Customers are affected by this incident
Public safety IS affected
This could have a negative affect to the public brand
Products/goods/ services are affected by this outbreak
Personnel safety IS NOT affected
Custom
Custom Factors
Request Packet Capture
Conduct Scans
Next Step


Prev Step
Define Risk Factors
Standard
IP is at risk of being exposed
Products/goods/services are affected by this outbreak
PII is at risk of being exposed
This act could be exploited for criminal activity
This could have a negative affect to the public brand
Customers are affected by this incident
Public safety is affected
Personnel safety is not affected
Custom
Business
Operational
Compliance
Custom Factors
Industry
Next Step



Prev Step

Identify the system(s) that have been affected

Servers

Desktop

Laptop

Mobile

VM

LDAP Directory

Identify the data compromised

Identify the IT services being impacted

Identify the means through which the malware gained access

Incident Database

Threat Database

Identify the vulnerabiity being exploited

Select Database

Vulnerability Logs

System Logs

Query Database

Generate Report

Identify how widespread the attack has spread

View Report

View Record Details

Select Records

Copy Record Details

Identify the tools used to detect the incident

SIEM

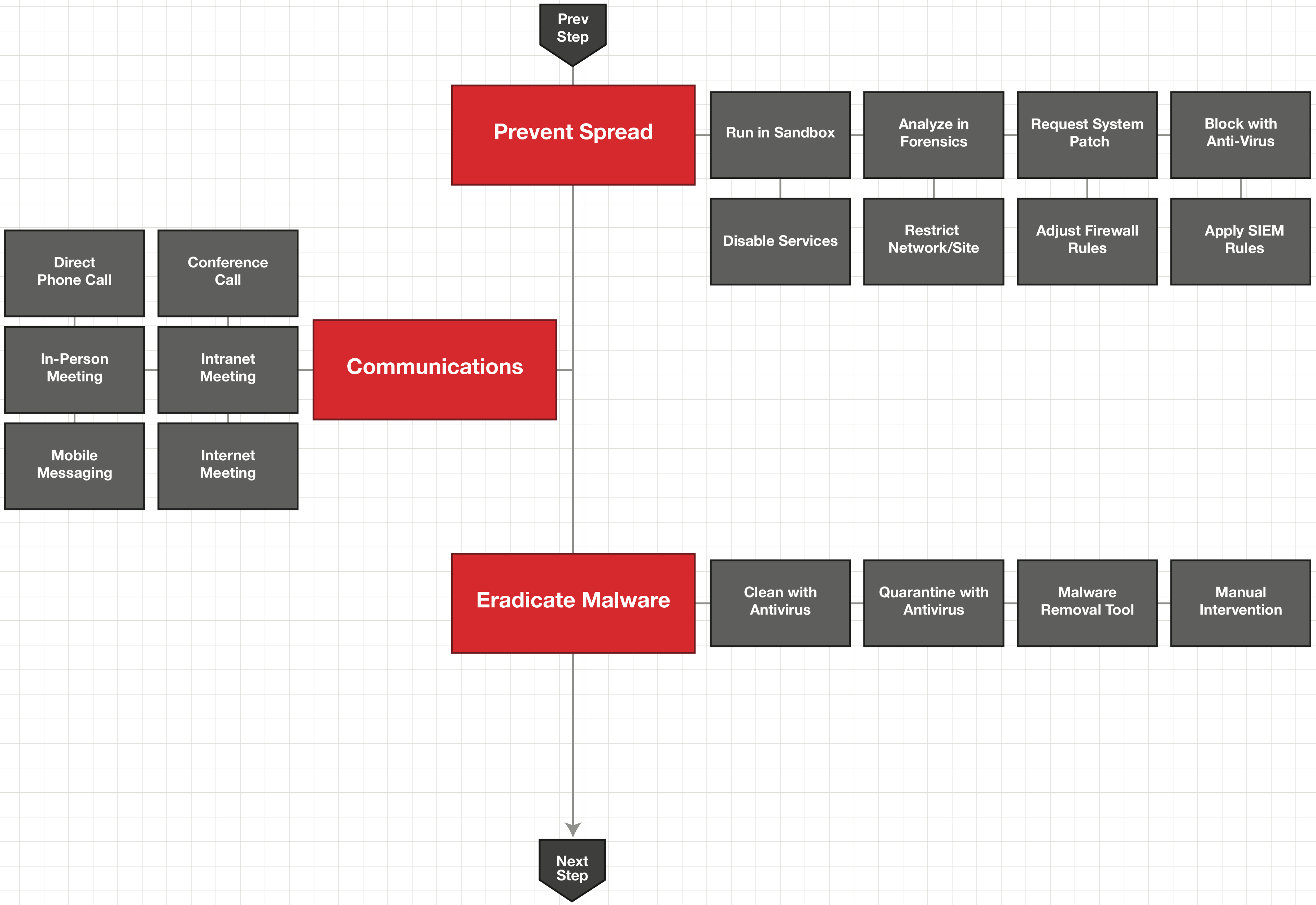
IDS

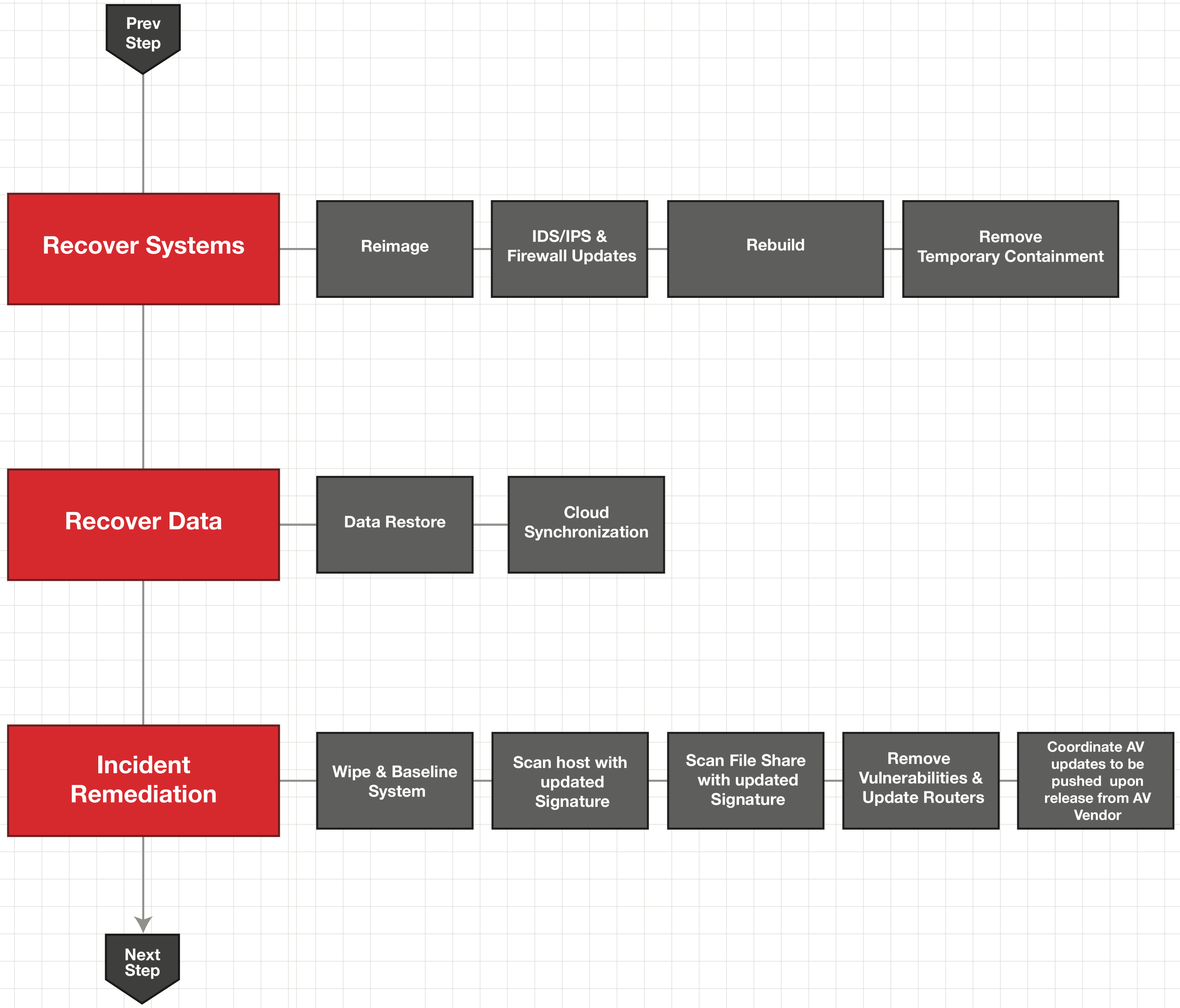
Firewall

Scanners

Antivirus

Next Step


Prev Step
Prevent Spread
Run in Sandbox
Analyze in Forensics
Request System Patch
Block with Anti-Virus
Disable Services
Restrict Network/Site
Adjust Firewall Rules
Apply SIEM Rules
Direct Phone Call
Conference Call
In-Person Meeting
Intranet Meeting
Communications
Mobile Messaging
Internet Meeting
Eradicate Malware
Clean with Antivirus
Quarantine with Antivirus
Malware Removal Tool
Manual Intervention
Next Step



Prev Step

Recover Systems

Reimage

IDS/IPS & Firewall Updates

Rebuild

Remove Temporary Containment

Recover Data

Data Restore

Cloud Synchronization

Incident Remediation

Wipe & Baseline System

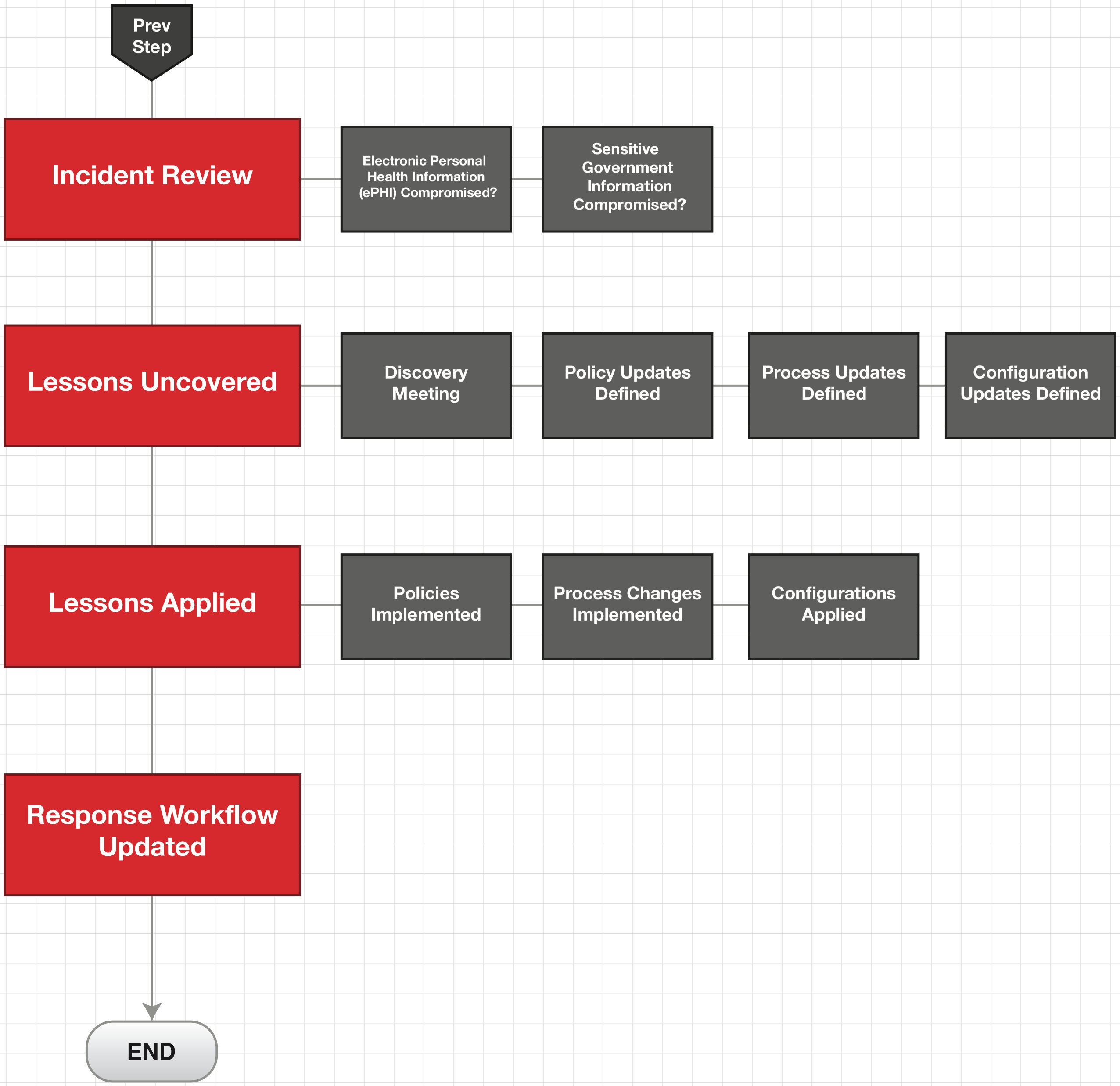
Scan host with updated Signature

Scan File Share with updated Signature

Remove Vulnerabilities & Update Routers

Coordinate AV updates to be pushed upon release from AV Vendor

Next Step



Prev Step

Incident Review

Electronic Personal Health Information (ePHI) Compromised?

Sensitive Government Information Compromised?

Lessons Uncovered

Discovery Meeting

Policy Updates Defined

Process Updates Defined

Configuration Updates Defined

Lessons Applied

Policies Implemented

Process Changes Implemented

Configurations Applied

Response Workflow Updated

END

Proactive Response

An automated playbook helps security teams optimize for efficiency and productivity. Your security team has the ability to analyze, detect and prioritize when all pertinent data and multiple security tools are integrated into one system. With one-screen visibility you can identify anomalies, assign tasks, access reporting and communicate across multiple departments effectively for quick responses.

Quick Containment

Time and speed are crucial in assessing the environment and risk in the context of your business. Playbooks give a complete view of the necessary tasks to capture the data needed to support proper recovery and forensics. The efficiency a playbook brings to a security team allows for quick responses to finding the source of the attack, following lateral movement across the organization and taking the proper steps mitigate damage.

Effective Remediation

Organization and automation are key benefits that result in effective remediation. Automated playbooks help to organize security processes, mitigation plans and smooth communication between multiple departments. By optimizing data collection, analysis, and communications you improve the odds for effective eradication, recovery with integrity and forensic-quality reporting.

Action Plan

Having a view into what is possible is the first step in taking action. The next step is to bring your team together to drive it toward reality. Email this guide to your peers and managers to begin sharing your playbook with them.

With this playbook, you will be better prepared to handle the response. To help with the management and automation of this incident response playbook, consider working with CyberSponse and their partners. Come take a look at **what they do**.

For additional incident response playbook examples, visit **https://www.incidentresponse.com/playbooks**

Security Management Benefits

- Be prepared to handle any incident your team faces
- Control the situation, minimizing the impact to the business
- Efficiently manage your response across multiple departments

Useful Links:

NIST Incident Handling Guide

SANS Incident Handler's Handbook

Risk Management Benefits

- Communicate effectively to ensure risk mitigation methods are applied
- Prioritize resources and activities where they matter most
- Report and tune based on response learning, reducing risk moving forward

Useful Links:

NIST Risk Management Framework Guide

Sample Policies and Plans

ABOUT FBI & -RELATED CYBERCRIME INVESTIGATION RESOURCES TO SUPPORT STATE & LOCAL LAW ENFORCEMENT

A number of FBI and FBI-related cybercrime investigation resources are available to support State and local law enforcement cybercrime investigations, including the resources described below.

The FBI Cyber Task Forces (CTFs), see attached Fact Sheet, https://www.fbi.gov/file-repository/cyber-task-forces-fact-sheet.pdf/.

The FBI has established a Cyber Task Force at each of the Bureau's 56 Field Offices. The FBI states their Mission as follows: in support of the national effort to counter threats posed by terrorist, nation-state, and criminal cyber actors, each CTF synchronizes domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions.

Within the Field Office territory, each CTF focuses on: Responding to cyber incidents and conducting victim-based investigations; Understanding and addressing the threats, vulnerabilities, and collection opportunities that exist, and Maintaining relationships and information sharing with key companies and institutions.

Each CTF also supports the national effort by, among other things, providing surge capability for cyber incidents outside of the territory and participating in national virtual teams on threats.

The FBI Regional Computer Forensics Laboratory (RCFL) Program, https://www.rcfl.gov/.

The RCFL Program is delivered through 17 Regional Computer Forensics Laboratories serving surrounding geographic service areas. The 17 RCFLs offer many of the types of technical services and technical training that will be useful to investigators of Cyber Native Crimes (see below). Each of the 17 RCFLs operates through the efforts of personnel seconded by Federal, State and local law enforcement agencies.

RCFL Service Offerings

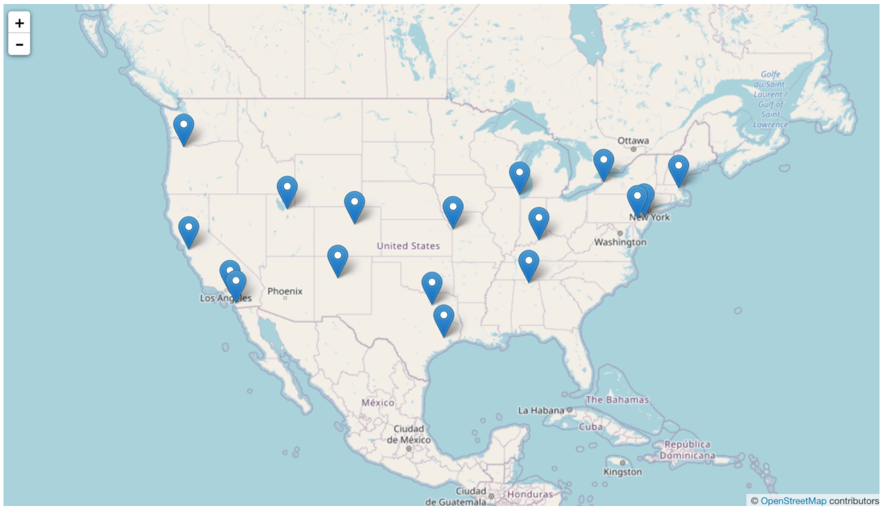
- Pre-Seizure Consultation
- Onsite Seizure and Collection
- Duplication, Storage, and Preservation of Digital Devices and Files
- Prompt, Accurate, and Impartial Forensics Examinations of Digitally Stored Media
- Courtroom Testimony
- Cell Phone Investigative Kiosk (CPIK)
- Loose Media Kiosk (LMK)

RCFL Training

- Case Agent Investigative Review (CAIR)
- Cell Phone Investigations
- Cell Phone Investigative Kiosk Training
- Loose Media Investigative Kiosk Training
- Mobile Device Forensics
- Seizing and Handling of Digital Evidence

RCFL Lab Locations

- Chicago
- Greater Houston
- Heart of America
- Intermountain West
- Kentucky
- New England
- New Jersey
- New Mexico
- North Texas
- Northwest
- Orange County
- Philadelphia
- Rocky Mountain
- San Diego
- Silicon Valley
- Tennessee Valley
- Western New York



SOURCE: https://www.rcfl.gov/service-areas

The National Cyber-Forensics Training Alliance (NCFTA), https://www.ncfta.net/.
A 501(c)(3) originally affiliated with the FBI, the NCFTA was formed as a "partnership between private industry, government and academia for the sole purpose of providing a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cyber crime."

The NCFTA specially focuses on utilization of the Internet for the sale of retail goods, including fraud related to e-commerce transactions and distribution of counterfeit merchandise, cyber threats to the financial services industry, and on providing actionable intelligence based on malware and technical threats.

Cyber Task Forces

Building alliances to improve the nation's cybersecurity

The threat posed by terrorists, nation-states, and criminal groups conducting computer network operations against the United States has escalated to the point that it is widely considered a top national security threat. Protective measures being implemented by critical infrastructure operators, safekeeping of intellectual property by industry, and vigilance by citizens can only go so far. Unlike crime problems that may affect a single city or region, cyber threats are inherently national threats. Federal, state, and local authorities, along with international partners, must synchronize efforts to aggressively counter them.

National coordination of cyber threat investigations…

The 2008 Comprehensive National Cybersecurity Initiative (CNCI) created the foundation for a whole-of-government approach to protecting the nation from cybersecurity threats. As part of the CNCI, the National Cyber Investigative Joint Task Force (NCIJTF) was established under Presidential Directive as one of the country's national cybersecurity centers. Located in the Washington, D.C. area, the FBI-led NCIJTF serves as the national focal point for coordinating cyber threat investigations. In its role as a headquarters-level task force environment, the NCIJTF enhances collaboration and integrates operations among the represented U.S. Intelligence Community and federal law enforcement partners against:

- Cyber terrorists exploiting vulnerabilities in critical infrastructure control systems
- Nation-state theft of intellectual property and trade secrets
- Financially-motivated criminals stealing money, identities, or committing cyber extortion
- Hactivists illegally targeting businesses and government services
- Insiders conducting theft and sabotage

…comes to your community.

While national-level coordination is important to securing the nation, teamwork at the local level is also essential. After more than a decade of combating cyber crime through a nationwide network of interagency task forces, the FBI has evolved its Cyber Task Forces (CTFs) in all 56 field offices to focus exclusively on cybersecurity threats. In addition to key law enforcement and homeland security agencies at the state and local level, each CTF partners many of the federal agencies that participate in the NCIJTF at the headquarters level. This promotes effective collaboration and deconfliction of efforts at both the local and national level. The CTF role within the field office territory includes:

- Responding to cyber incidents and conducting victim-based investigations
- Understanding and addressing the threats, vulnerabilities, and collection opportunities that exist
- Maintaining relationships and information sharing with key companies and institutions

Each CTF also supports the national effort by:

- Providing surge capability for cyber incidents outside of the territory
- Participating in national virtual teams on a topic or threat
- Contributing subject matter experts for instruction, presentations, and research/development projects

CTF Mission

In support of the national effort to counter threats posed by terrorist, nation-state, and criminal cyber actors, each CTF synchronizes domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions.

Join us in partnering for a more secure future.

Successfully countering threats to the nation's cybersecurity requires a multi-disciplinary and multi-stakeholder team approach, and your local CTF values your contribution. By participating in the CTF, your agency's mission will be enhanced through:

Understanding the Threat

The threat landscape is constantly changing, and what your agency doesn't know can hurt those you are dedicated to protecting. By joining the CTF, your personnel will have access to real-time classified reporting.

Training Opportunities

Participants gain access to the FBI's cyber investigations curriculum, comprised of dozens of internally-developed and industry certification courses.

Access to Resources

For state and local partners, officer overtime, lease vehicles, fuel, smart phones, and computer equipment are available.

For more information, contact your nearby FBI field office or visit www.fbi.gov.

Introduction to RCFLs

INTRODUCTION

Digital forensics is the application of science and engineering to the recovery of digital evidence in a legally acceptable method. Digital Forensics Examiners use digital investigation and analysis techniques to determine potential legal evidence by applying their skills on a variety of electronic devices, software programs, different operating systems, varying hard drive sizes, and technologies.

A Regional Computer Forensics Laboratory (RCFL) is a digital forensics laboratory and training center devoted to the examination of digital evidence in support of criminal investigations and to the detection and prevention of terrorist acts. The first RCFL was established in San Diego, California in 1999, and began as a cooperative effort between the FBI and other federal, state, and local law enforcement agencies to address digital evidence. The RCFL Program is based on this model of partnership between the FBI and other law enforcement agencies at the federal, state, and local levels operating within a geographic area.

THE RCFL NETWORK

In addition to the San Diego RCFL, RCFLs are operating in Albuquerque, New Mexico; Boston, Massachusetts; Buffalo, New York; Centennial, Colorado; Chicago, Illinois; Dallas, Texas; Hamilton, New Jersey; Huntsville, Alabama; Houston, Texas; Kansas City, Missouri; Louisville, Kentucky; Menlo Park, California; Orange, California; Philadelphia, Pennsylvania; Portland, Oregon; and, Salt Lake City, Utah.

KEY GOALS

The key goals of the RCFL Program are to—

- Provide timely, professional and technically advanced digital forensic services to the law enforcement agencies in an RCFL’s service area.
- Fully utilize applied science and engineering capabilities to support digital forensic examinations.
- Increase the confidence of investigators, prosecutors, and judges in the digital forensics examination discipline through standardized training and forensic protocols.
- Provide responsive and flexible services in support of diverse investigative programs.
- Meet legal and administrative requirements of diverse judicial systems.

Introduction to RCFLs

REQUESTING DIGITAL FORENSICS SUPPORT

Each RCFL evaluates requests for direct technical support on a case-by-case basis and provides services (regardless of agency) based upon established priorities. RCFL staff members may travel to crime scenes or participate in executing search warrants.

STAFFING

An RCFL is equipped and staffed to recover evidence from original electronic equipment or backups of computer data. The RCFL can also acquire evidence from a crime scene or search site. By doing so, evidence can be removed and brought to the RCFL for further examination. A typical RCFL consists of a Director; 10-12 Examiners; and an administrative support person.

FORENSICS RESPONSIBILITIES

The primary forensics responsibilities of an RCFL are to—

- Conduct a comprehensive examination of digital evidence
- Provide a complete and timely report to the contributor
- Provide testimony as needed
- Act as a regional focal point for digital evidence issues.

OPERATIONAL SUPPORT RESPONSIBILITIES

The RCFLs provide operational support in the following ways—

- Providing advice on wording for search warrants to recover digital evidence
- Gathering intelligence in preparation for writing a warrant
- Sharing on-site technical assistance with investigators executing the warrant
- Providing advice for seizure of digital evidence or acquiring copies of data at the search warrant site.

For more information, contact the National Program Office:

703.985.3677 npo@rcfl.gov www.rcfl.gov

Benefits of Participation

INTRODUCTION

A Regional Computer Forensics Laboratory (RCFL) is a computer forensics laboratory and training center that is devoted entirely to the examination of digital evidence in support of criminal investigations, such as, but not limited to—

- Terrorism
- Murder
- Child pornography/crimes against children
- Crimes of violence
- The theft or destruction of intellectual property
- Financial, property, or Internet crimes
- Fraud
- Trade secret theft.

RCFLS BENEFIT LOCAL LAW ENFORCEMENT

An RCFL is a partnership between the FBI and other law enforcement agencies operating within a geographic region. Organizations that enter into a Memorandum of Understanding with the FBI become participating agencies in the RCFL. In this capacity, they detail staff members to staff the laboratory, and in return, they and their personnel receive—

- Access to digital forensics examination and advisory services
- Seven weeks of the same sophisticated technical training that is provided to FBI's certified computer forensics Examiners
- Compensation of any overtime worked
- Exposure to the most technologically advanced computer equipment available. The FBI invests an estimated $26,000 per workstation and updates the equipment approximately every two years
- Broad experience in a variety of digital forensics cases
- An RCFL-issued cell phone and use of a government-leased vehicle
- A stake in the management of the RCFL.

TRAINING IS KEY

RCFL detailees receive the same training and certification that is provided to the FBI's Computer Analysis Response Team (CART). Many RCFL Examiners cite the opportunity to obtain the prestigious CART certification and follow-on training as one of the greatest benefits of joining the Program. The FBI invests an average of $13,000 in their first year and $10,000 in the second year per new Examiner.

Benefits of Participation

THE NEED FOR COMPUTER FORENSICS EXPERTISE CONTINUES TO RISE

The RCFL Program represents a national effort to use digital evidence to prosecute white-collar and violent crimes. Today, RCFLs are available to over 4,000 law enforcement agencies spanning 17 states with locations in Albuquerque, New Mexico; Buffalo, New York; Centennial, Colorado; Chicago, Illinois; Dallas, Texas; Dayton, Ohio; Hamilton, New Jersey; Houston, Texas; Kansas City, Missouri; Louisville, Kentucky; Menlo Park, California; Orange, California; Philadelphia, Pennsylvania; Portland, Oregon; Salt Lake City, Utah, and; San Diego, California.

The widespread use of computers has led to an increasing number of cases in which digital media is presented as evidence. In Fiscal Year 2012, the RCFL Program achieved the following accomplishments —

- Received **5,060** requests for service
- Conducted **8,566** digital forensics examinations
- Trained **6,500** law enforcement personnel
- Processed **5,986** TB of data
- Provided assistance in **553** onsite operations conducted by law enforcement

For more information, contact the National Program Office:

💬 703.985.3677 @ npo@rcfl.gov 🌐 www.rcfl.gov

TAB E

E. APPENDICES

E.1 NSA RESOLUTION OF SUPPORT, 2018-07

E.2 NSA RESOLUTION OF SUPPORT, 2019-09

E.3 PERF POLICE EXECUTIVE REPORT ON THE NYPD PILOT PROGRAM, APRIL 8, 2021

2018-07

NSA ADOPTS THE NSA NATIONAL LAW ENFORCEMENT CYBER INVESTIGATORS PROGRAM, TRAINED & CERTIFIED BY NSA.

WHEREAS, cybercrime is out of control, and the Nation's Sheriffs, their law enforcement partners, and U.S. policymakers must do more to combat the global cyber threat;

WHEREAS, the NSA Homeland Security Committee's Cybersecurity and Crime Work Group, Chaired by Sheriff David Goad (Ret.), and whose members include sheriffs and deputies, state and local police, prosecutors, and private sector firms, has been working diligently on developing approaches and solutions that can be executed upon by the nation's sheriffs, working in and through the NSA, to make a difference in combatting the cyberthreat, and is focused especially on NSA Training and Certification Programs that can aid sheriffs and their partners in investigating and prosecuting cybercrimes, and in making sheriffs' Offices more cybersecure;

WHEREAS, the Work Group has developed and presented to the Homeland Security Committee, and the Homeland Security Committee has approved and recommended, a Plan for the NSA Law Enforcement Cyber Investigators Program, Led by the Nation's Sheriffs and Trained and Certified by NSA, to launch the NSA Law Enforcement Cyber Investigators Program led by Sheriffs and Deputies, to investigate and support prosecution of cybercrimes, and to advance five priorities:

- NSA Training, especially through the NSA Institute for Cyber Security;
- NSA Certification of Law Enforcement Cyber Investigators (NSA Institute for Cyber Security);
- Outreach to Sheriffs & Deputies in Building A National Network of Law Enforcement Cyber Investigators;
- Development and Maintenance of A Shared Cybercrime Resources Database; and
- Development of A National Network of Law Enforcement Cyber Investigators.

NOW THEREFORE, **BE IT RESOLVED,** that, in order to more deeply engage the Nation's Sheriffs and Deputies in the investigation and prosecution of cybercrimes and to step up the law enforcement response to cybercrime and the cyber threat, the National Sheriffs' Association hereby supports and adopts the NSA Law Enforcement Cyber Investigators Program;

AND, BE IT FURTHER RESOLVED, that the National Sheriffs' Association urges the Nation's Sheriffs and Deputies, Sheriffs' partners in municipal, State and Federal police, the Nation's prosecutors, Sheriffs' partners in Federal Agencies and International Police Organizations, and the Nation's cybercrime investigators in public agencies and in private firms, to join with the Nation's Sheriffs in working collaboratively to make a material difference in stemming the cyberthreat facing the Nation, by more effectively combatting cybercrime through the NSA Law Enforcement Cyber Investigators Program.

Approved by the Board of Directors of the National Sheriffs' Association on June 18, 2018, at the Annual Conference of the National Sheriffs' Association, New Orleans, Louisiana. This resolution to remain in effect until June 24, 2022, in accordance with Article XIII, Section 6 of the Constitution and Bylaws of the National Sheriffs' Association.

2019-09

NATIONAL SHERIFFS' ASSOCIATION SUPPORTS THE NSA CYBERCRIME INVESTIGATOR'S PROGRAM'S ENGAGEMENT WITH NW3C, DOD, U.S. ATTORNEYS AND PRIVATE SECTOR PARTNERS

WHEREAS, by NSA Resolution 2018-07, the National Sheriff's Association ("NSA") expressed its support for a National Law Enforcement Cybercrime Investigator's Program, led by Sheriffs, aimed at more deeply engaging the Nation's Sheriffs and Deputies in the investigation and prosecution of cybercrimes and at stepping up the law enforcement response to cybercrime and the cyber threat (the "Program");

WHEREAS, the Program is built around three essential Program components—a Cybercrime Investigator's Shared Resource Database, a Cybercrime Investigator's Information Sharing Environment, and Cybercrime Investigator Training and Certification by NSA—and also upon collaboration between the Nation's Sheriffs, other local and State law enforcement (including prosecutors), and cybercrime investigators in the private sector and in military and other Federal agencies;

WHEREAS, the NSA Cybersecurity & Crime Work Group ("NSA Work Group"), led by Sheriff David Goad, Ret., which originally developed and published the concepts underlying the Program, has pushed forward with efforts to develop, implement and fund the Program's essential components through strategic partnerships with, among others, the U.S. Department of Defense, including the National Guard, the U.S. Attorneys' Offices, and vetted and trusted private sector cybercrime investigators;

WHEREAS, the National White Collar Crime Center ("NW3C"), a 501(c)(3) entity that provides a nationwide support system for law enforcement and regulatory agencies tasked with the prevention, investigation and prosecution of economic and high-tech crime, is a Member of the Work Group and, in collaboration with the Work Group, has developed its "CCCE" (Certified Cyber Crime Examiner) certification for public and private cybercrime investigators that "attests to the holder's knowledge of proper digital forensic techniques and best practices for working with digital evidence", which CCCE Certification is being proposed as the first concrete step forward for the Program and its Training & Certification component;

NOW THEREFORE, BE IT RESOLVED that the NSA supports NW3C's "CCCE" (Certified Cyber Crime Examiner) certification for incorporation into NSA's Cybercrime Investigator's

Program, and congratulates the Work Group and NW3C for having taken the first concrete step in implementing the Program; and

BE IT FURTHER RESOLVED, that the NSA supports engagement with the Program by the U.S. Department of Defense, including the National Guard, and U.S. Attorneys' Offices, as well as by vetted and trusted private sector cybercrime investigators.

This resolution was adopted by the membership of the National Sheriffs' Association on June 18, 2019, at the Annual Conference of the National Sheriffs' Association, in Louisville, Kentucky. The resolution shall remain in effect until June 18, 2023, in accordance with Article XIII, Section 6, of the Constitution and Bylaws of the National Sheriffs' Association.

When individuals fall victim to cybercrime, they often report the offense to their local police department. But most police officers lack the knowledge or tools to respond in a meaningful way. In 2019, the New York City Police Department implemented a pilot program to help its officers respond to the typical cybercrime complaints they receive.

The pilot program was for "cyber-enabled" crimes, as opposed to "cyber-native" crimes. Ravi Satkalmi, Deputy Director for Intelligence Analysis at the NYPD, explained the difference:

*"**Cyber-enabled crimes** are traditional crimes that now have a new mode for delivery. They might be committed online, though social media, or through cell phones, but they're still traditional crimes."*

For example, cyber-enabled crimes include financial frauds that are carried out with digital technology, identity theft, purchase of illegal drugs online, phishing and pharming scams in which victims are tricked into releasing personal or financial information through fake emails or websites purporting to be legitimate banks or other businesses, and many other types of crime.

*"**Cyber-native crimes** are those that can only be committed because we have these tools. They didn't necessarily exist as crimes before these tools were available."*

Cyber-native crimes include crimes in which a computer or other digital system is the target of the attack as well as the means of the attack, such as malware attacks, and hacking of government agencies' or corporate databases.

PERF spoke with five current and former members of the NYPD to learn more about the pilot program and other steps they are taking to address cybercrime.

THE CHALLENGE POSED BY CYBERCRIME

Deputy Chief John Hart, Intelligence Bureau

The recent FBI IC3 report showed a 69% increase in total internet crime complaints from 2019 to 2020. I don't think that's just due to COVID; I think there's also better reporting of these crimes.

Announcements

Click here to view PERF's April 15th webinar: *Managing Demonstrations: New Strategies for Protecting Protesters and the Police*

Click here to read past editions of "*Trending,*" PERF's weekly email update to its members, including the most recent: "What If the Police Shared Ownership for Managing Demonstrations with the Community?"

However, we're still just scratching the surface of what's out there. And the FBI only has the ability to investigate a very small portion of those complaints. That's not a criticism, it's just a fact.

The DHS Cybersecurity and Infrastructure Security Agency (CISA) is doing a great job helping state and local law enforcement as well. But ultimately we all have to become better at this.

We had done a pilot cybercrime program at the end of 2019. We released the report at the beginning of 2020, but then all our energy and time went into COVID and police reform. I think we learned some important lessons from the pilot, and we want to work with all our partners on how we can better handle these cases.

The FBI looks at two things when deciding whether to take a cybercrime case. One is if it meets a certain dollar threshold. The other is whether it's committed by nation-state actors, rather than local criminals. Those two things separate us and our federal partners in all crime. It's important for us to know where that separation is, what they do, and what we should be doing at a local level.

But I know that patrol cops everywhere are not equipped to handle these crimes. They say, "It's cyber, so I don't know what to do. Let me pass it on to someone in my agency who's a specialist."

THE PILOT PROGRAM

Nick Selby, former Director of Cyber Intelligence and Investigations

When we started the pilot, there was skeptical questioning about whether the patrol cops would be interested. But after training more than 700 patrol officers in New York, I can tell you that they're very frustrated. Many of them have family members who have been victims of scams on their computers and phones, and we see it on the news and hear it from the community outreach workers and the Grand Larceny Division. So they're very aware of these crimes, but they just haven't been given the tools and training to handle them.

And the cyber special agents at the FBI are brilliant, but to ask them to look at a crank phone call where someone lost $6,000 is like asking Mick Jagger to do the sound check at a Rolling Stones concert. They're very busy with very complex things. So there should be some way to fill the gap below that threshold.

Working with Deputy Chief Hart, Chief Thomas Galati, Deputy Commissioner John Miller, then-Commissioner James O'Neill, and Assistant Commissioner Rebecca Weiner, we saw the problem of cybercrime as one where we just didn't know what the answers were. We didn't know the most common scams, who was getting scammed, or where they were getting scammed. For the NYPD, an agency that measures almost everything, that was unacceptable.

In early 2019, Commissioner O'Neill and Deputy Commissioner Miller gave me the mandate to start looking at this. Because we weren't measuring these crimes, we had to scan our records management system, and look at millions of calls to find the calls that look like cybercrime. Those cybercrimes are things like fraudulent phone calls, bank account takeovers by someone who fraudulently obtains the password, and phones being taken over through "SIM swapping." This group of cybercrimes would not include things like ransomware, critical infrastructure attacks, or nation-state attacks.

Over the course of the first six months of 2019, we searched diligently for cases that looked like what we wanted to focus on. Using that information, we estimated that in 2018 there were about $230 million worth of these kinds of cybercrimes in New York City. That's big, because during that same period, car thefts totaled about $50 million in New York City.

We presented this information and asked for the resources to do a pilot program. Everyone agreed this was worth trying. We decided to do it in Queens South, because we wanted a place that was busy enough to get significant numbers, but not so busy that we might get in the way of more serious investigations. We got help from the Queens District Attorney's cyber unit, and by the second half of 2019, we were ready to start.

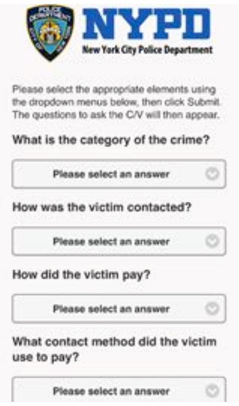
We created a 15-minute training program that educated cops about cyber-enabled crimes. Over the course of three months, we trained about 700 officers.

And every NYPD officer has an iPhone, so we leveraged that resource. We built an app that allowed officers to collect basic information about the type of crime and how it was carried out. Using the app, officers have to answer four questions in a drop-down box:

- What is the category of the crime?
- How was the victim contacted?
- How did the victim pay?
- What contact method did the victim use to pay?

Once they answered the four questions, the app gives them questions to ask the complainant.

The point of the pilot was to teach patrol officers how to gather the key information and write it down, so that the detectives had usable leads to follow when they received the cases.



NYPD
New York City Police Department

Please select the appropriate elements using the dropdown menus below, then click Submit. The questions to ask the C/V will then appear.

What is the category of the crime?

Please select an answer

How was the victim contacted?

Please select an answer

How did the victim pay?

Please select an answer

What contact method did the victim use to pay?

Please select an answer

A friend and I developed the app ourselves, and we have made it open and free to all law enforcement and no one else. I've already distributed it to several small agencies.

One of the first calls I went to was a kid in Queens who had sold his iPhone on eBay, and had left an intimate video on that phone. The person who bought that phone tried to extort him for $1,000, saying that otherwise the video would be posted on Facebook. The kid was very upset and called the police.

To investigate a case like that, you don't need any forensics. Somebody just had to send a subpoena to eBay and ask who bought the phone. It's quite simple.

But it never gets to that point if the cops don't ask the right questions. The app and the training helped them ask the right questions.

Over the course of the pilot, we found a couple interesting things. First, our estimate of the costs of these crimes rose to $329 million in 2019.

The second thing we learned is that the demographic profile of victims is across the board. The median age of victims who reported their crime was 42. Older people tended to fall for scams like, "Your nephew is in jail, and you have to send bail money for him." Younger people tended to be victims of extortion, like that kid in Queens. But the demography was evenly spread. Whether you're black or white, rich or poor, it affects everyone in the city.

Deputy Chief Hart

The training, the app, and the presence of the pilot led to much better initial reports. Most cops understood what they were doing. During the pilot program, 60% of the reports had the right terminology and the right details. And 90% of the cops who responded to these types of calls used the app, which I think is a significant accomplishment. We gave them a tool, and they made use of it right away.

We put this out, then everything came to a screeching halt a year ago with COVID. So we don't have as much information about arrests, though we know about some isolated successes. Now we want to get back to focusing on this.

TRAINING

Christina Soto, Intelligence Research Specialist

We started training officers through this pilot program. We started by defining cybercrime, because they often don't know the definition. We explained the categories of complaints. We provided a 1-800 number they could call with questions, and gave them the app. These resources allow them to feel comfortable with these complaints and know that someone in the department is looking at them. After the training, they were much more receptive toward the pilot program.

Deputy Chief Hart

We trained every cop on every patrol tour in every command in Queens South. We wanted to hit all the cops with a short, pointed training at their roll calls. This was 15 minutes in person, in front of the roll call.

IMPLEMENTATION IN SMALLER AGENCIES

Deputy Chief Hart

There's nothing to stop this from being implemented in smaller agencies. Whatever your size, you have trainers. It's not so complex that a local trainer can't teach it in an effective manner.

It helps to have a resource for cops to reach out and ask questions in the moment, whether that's a fusion center or something else. That's one area where it may be harder for a smaller agency to find the resources. But our whole team for this was only about six people.

Christina Soto

Agencies of any size can have analysts review their data for key words to identify hot spots and trends. Agencies can also start training officers at the academy. That training could include defining cybercrime, which types of complaints constitute a cybercrime, and what they should do when they receive a cybercrime complaint.

ADDRESSING CYBER-NATIVE CRIMES

Ravi Satkalmi, Deputy Director for Intelligence Analysis

The NYPD is looking to improve on the intelligence aspect of this problem. For both cyber-enabled and cyber-native crimes, we're learning what the threats look like and coming up with the program to respond to the threats.

Our Intelligence Bureau is closely working with our Information Technology Bureau, which is doing the front-line defense. We're speaking with them on a daily basis to look at the kinds of cyber-native threats toward the NYPD and its systems. That might be people trying to make unauthorized intrusions or a denial-of-service attack. We want to get a sense on who those actors are, how prolific they are, and the danger they present.

We're looking at a range of actors. At the top level, we have highly publicized attacks from nation-states against American entities in government and law enforcement. We also have amateurish folks who go online, purchase malware, and deploy it against a target. That's becoming easier, and we want to understand how we can respond to that.

Lieutenant Gus Rodriguez, Intelligence Bureau

A few detectives and I are assigned to a cyberterrorism squad within the New York City FBI Office's cybercrime task force. We have a guiding question: In the cyber realm, how do we proactively protect the 17 sectors of critical infrastructure that make New York City move? Those sectors include the Department of Environmental Protection, which pumps 1.1 billion gallons of water into the city every day; the Metropolitan Transit Authority, which runs our 26 train lines; and the Department of Transportation, which makes sure our 13,000 traffic lights are working.

Working with those sectors, we realized we needed to pass information about malware we were seeing on to the NYPD's Information Technology Bureau, which has to make sure we respond to 25,000 9-1-1 calls a day. We see the threats day-in and day-out, and we have to make sure that information gets to the NYPD and the other 120 agencies in the city.

MOVING FORWARD

Deputy Chief Hart

This problem is real, and it’s affecting our citizens, not far-off places. It’s a large amount of money. And we can make a difference if we train our people the right way and give them the right tools.

NPR reported on the pilot program, and we've written a full internal report on the program.

The PERF Critical Issues Report is part of the Critical Issues in Policing project, supported by the Motorola Solutions Foundation.

MOTOROLA SOLUTIONS FOUNDATION

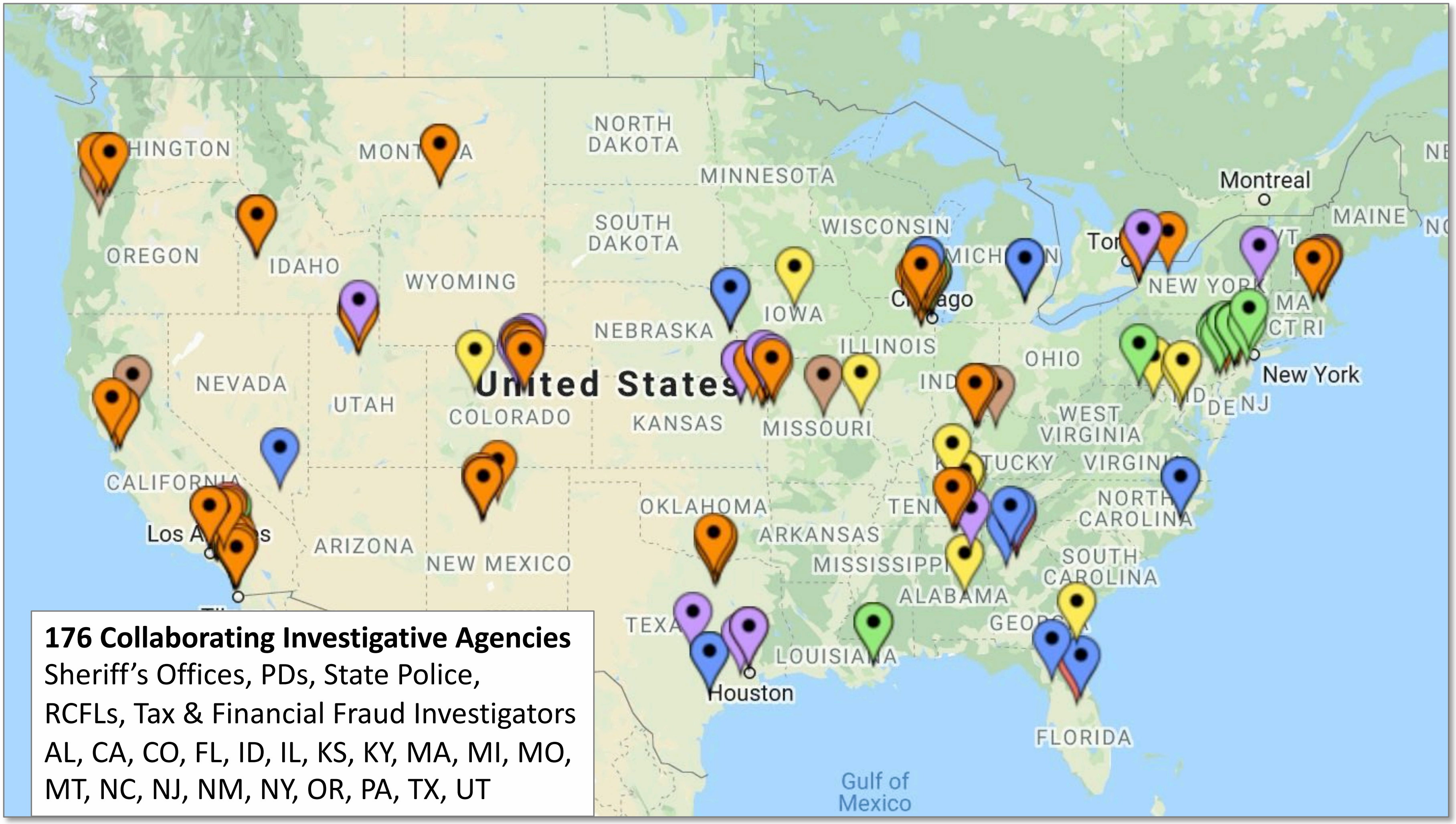
PERF also is grateful to the Howard G. Buffett Foundation for supporting this work.

THE HOWARD G. BUFFETT FOUNDATION

© Police Executive Research Forum
1120 Connecticut Ave. NW Suite 930 Washington, DC 20036
(202) 466-7820

Back to top

Proposed NCIP/RCFL Local Law Enforcement Collaboration



176 Collaborating Investigative Agencies
Sheriff’s Offices, PDs, State Police,
RCFLs, Tax & Financial Fraud Investigators
AL, CA, CO, FL, ID, IL, KS, KY, MA, MI, MO,
MT, NC, NJ, NM, NY, OR, PA, TX, UT