



Guide for Conducting Cyber Investigations Using NCIP Tools:

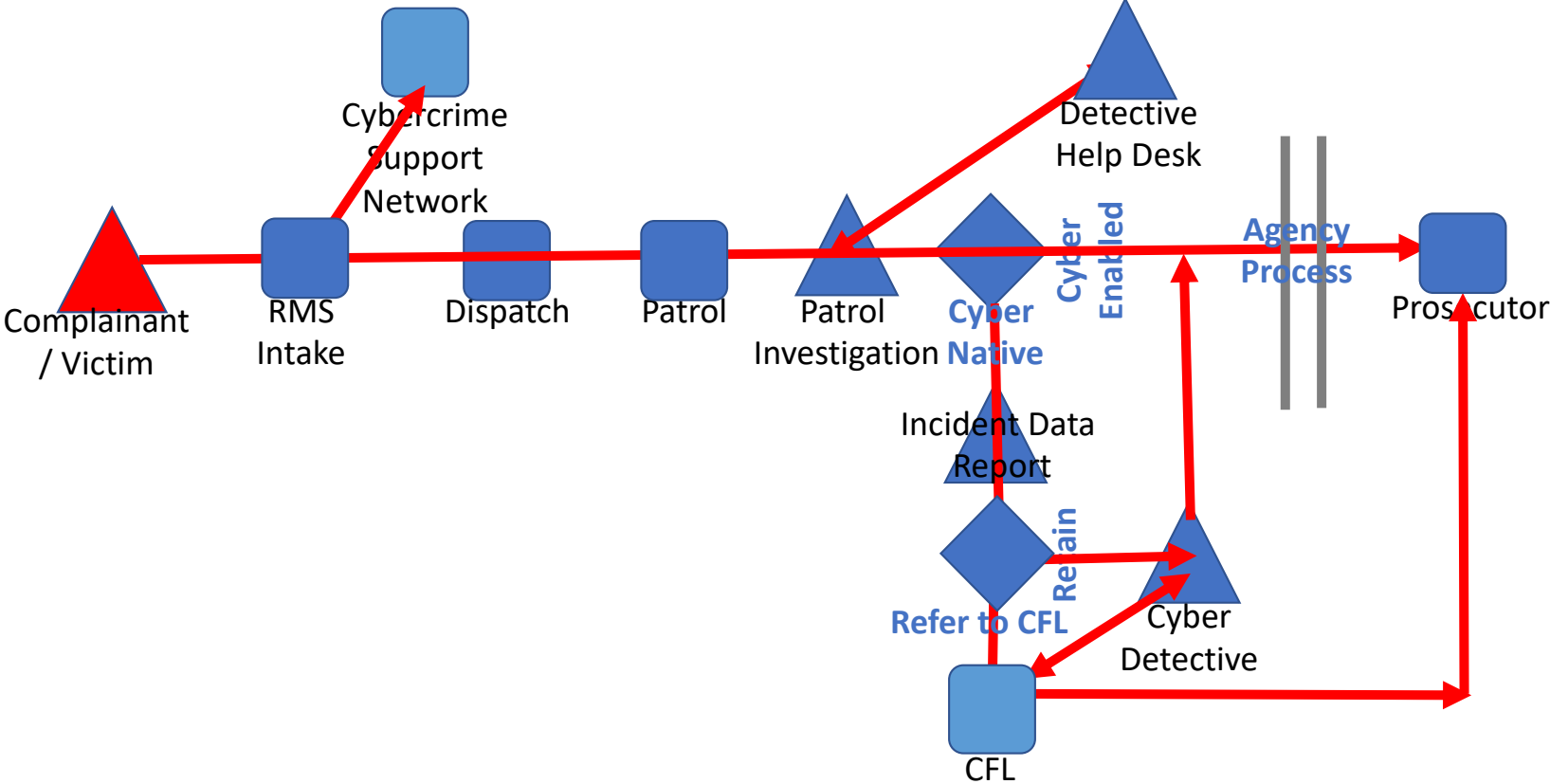
*Blazing a Path For
Local Law Enforcement's Future*

**A Guide For Sheriffs and Chiefs
NSA Annual Conference, Phoenix
June 2021**

About NCIP

- 2021 Goal: provide pre-packaged tools and a clear path forward for Sheriffs, Chiefs & Prosecutors 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
- Special Thanks to NYPD Deputy Chief John Hart and Nick Selby, former NYPD Director of Cyber Intelligence and Investigations, for their thought leadership on Cyber Policing

Cyber Investigations Flow Chart, Powered by NCIP-provided Tools



Cyber Investigation Tools Provided to Law Enforcement, Most for No or Nominal Charge

***Cybercrime Victim Support**, provided by Cybercrime Support Network: No Charge

***Training & Training Materials, & Cyber Enabled App**: No Charge

***CFL Cyber Incident Data Report Processes & Forms**: No Charge

***Cyber Native App**: No charge to Law Enforcement Agencies (in development)

****NCIP Forum**: Nominal (Sustainment) charge to Law Enforcement Investigators

*****CFL Cyber Incident Investigation Services**: As quoted and agreed

Cyber Enabled Crime OR Cyber Native Crime?

- **Cyber Enabled Crime: traditional criminal activity (e.g., fraud, scams) that simply use computers/devices/networks to commit the crime**
 - Can be investigated by Non-Technical Officers from Complaint to Charging Decision using familiar investigative processes and tools
 - Nothing new here
- **Cyber Native Crime: new types of crimes that cannot be committed without computers/devices/networks (e.g., Ransomware, Hacking, Denial of Service attacks)**
 - **First Step**—preparing Cyber Forensic Lab (CFL) Incident Data Report; can be done by minimally technical agency personnel
 - Note: Simply Completing & Sharing Cyber Forensic Lab Incident Data Report creates value for many other Investigations
 - **Second Step**—Conducting Cyber Native Investigation to Charging Decision—needs new tools & Technically Proficient Cyber Investigator
 - Cyber Native Investigation can be done internally by **Cyber Detective**, or via regional Cyber Task Force OR referred to CFL, your State's FBI Cyber Task Force, or others

Cyber Enabled Investigations Non-Technical Training Materials & App



NCIP Non-Technical Cyber Enabled Investigations Program (CEIP): Overview on Cyber Enabled Crime

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


April 2021



Built on Training Concepts Developed by NYPD

**Developed by
Nick Selby &
Raven Zachary**

Cyber Native Investigations: Driven by Incident Data Reports & App



National Cybercrime Investigators Program
CFL Form 1: Forensic Incident Data Report

This Form 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. Prosecutor Address			29. Prosecutor Email		
30. Subject's Name			31. Subject's DOB		
32. Deceased/Victim Name		33. Victim Is a Minor <input type="checkbox"/>	34. Victim's DOB	35. Relevant Dates	
36. Needed Service Type			37. Associated Case(s)		
38. Is new evidence being provided today? <input type="checkbox"/>	39. Has any other person accessed the evidence? (provide details)				
40. Additional Comments					

41. Check all items attached to this document:

<input type="checkbox"/> Confession/statement from accused	<input type="checkbox"/> Photo of victim
<input type="checkbox"/> Witness Statement.	<input type="checkbox"/> Photo of subject
<input type="checkbox"/> Charge Sheets	<input type="checkbox"/> Defense expert Info
<input type="checkbox"/> Report for related Online Investigation	<input type="checkbox"/> Prior forensic analysis

NCIP/CFL Form 1 v1.0 info@ncip.tech 504-717-4872

Program Report
 Digital Media Recovery for
 prosecution support

data for further investigation.

ALTERNATE

Indicator:

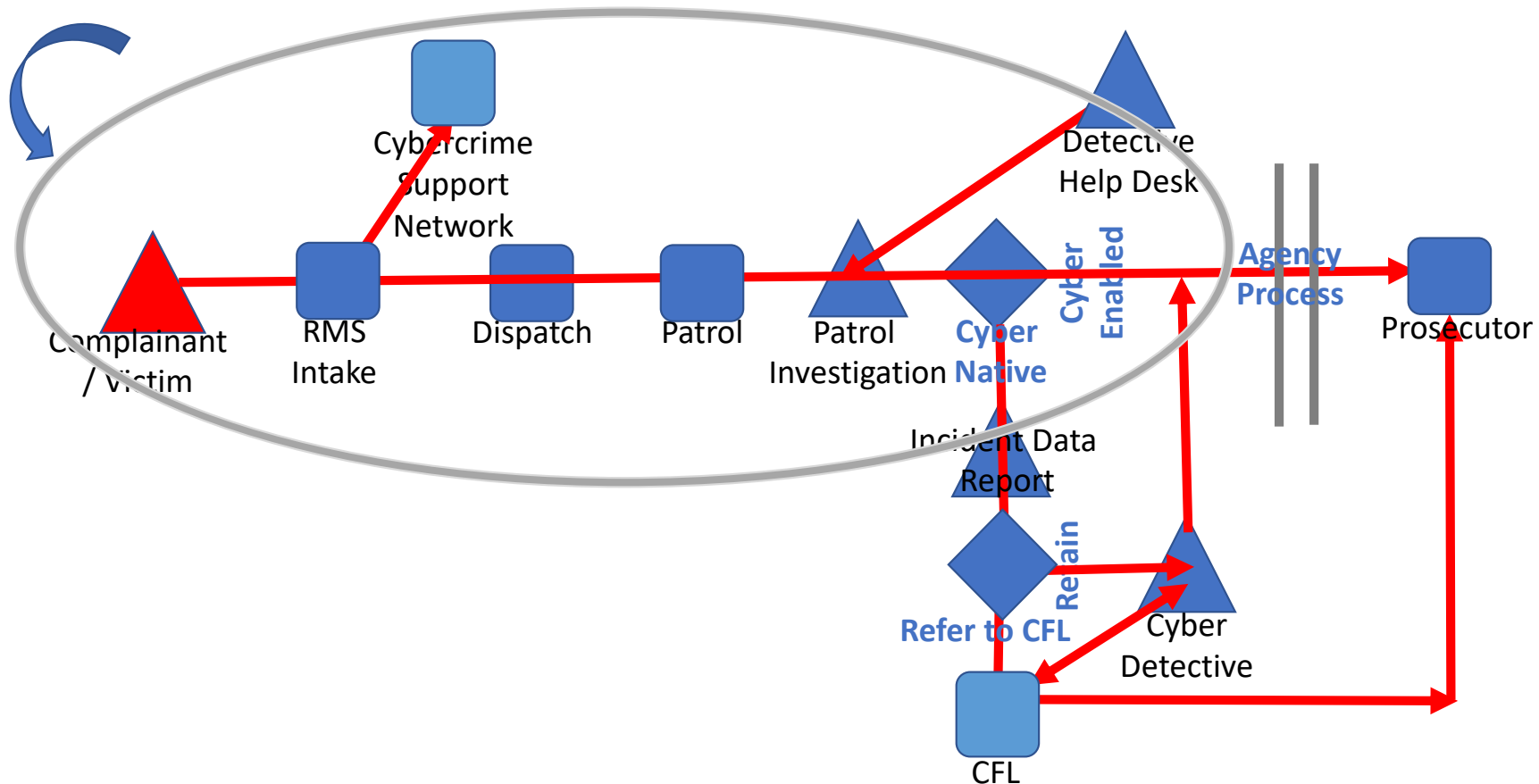
PROSECUTOR

1

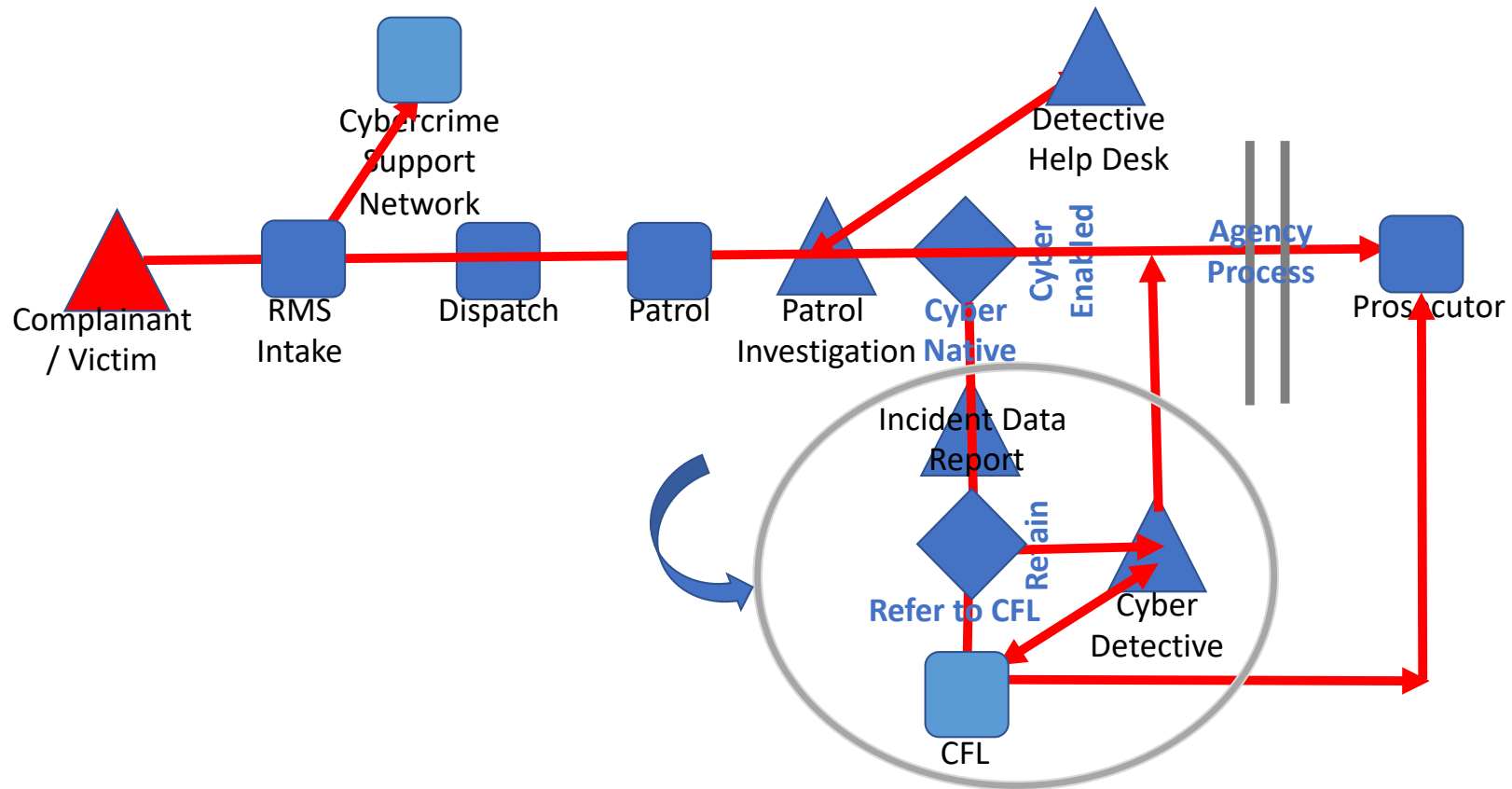
Cyber Native App
In Development

Developed by NCIP

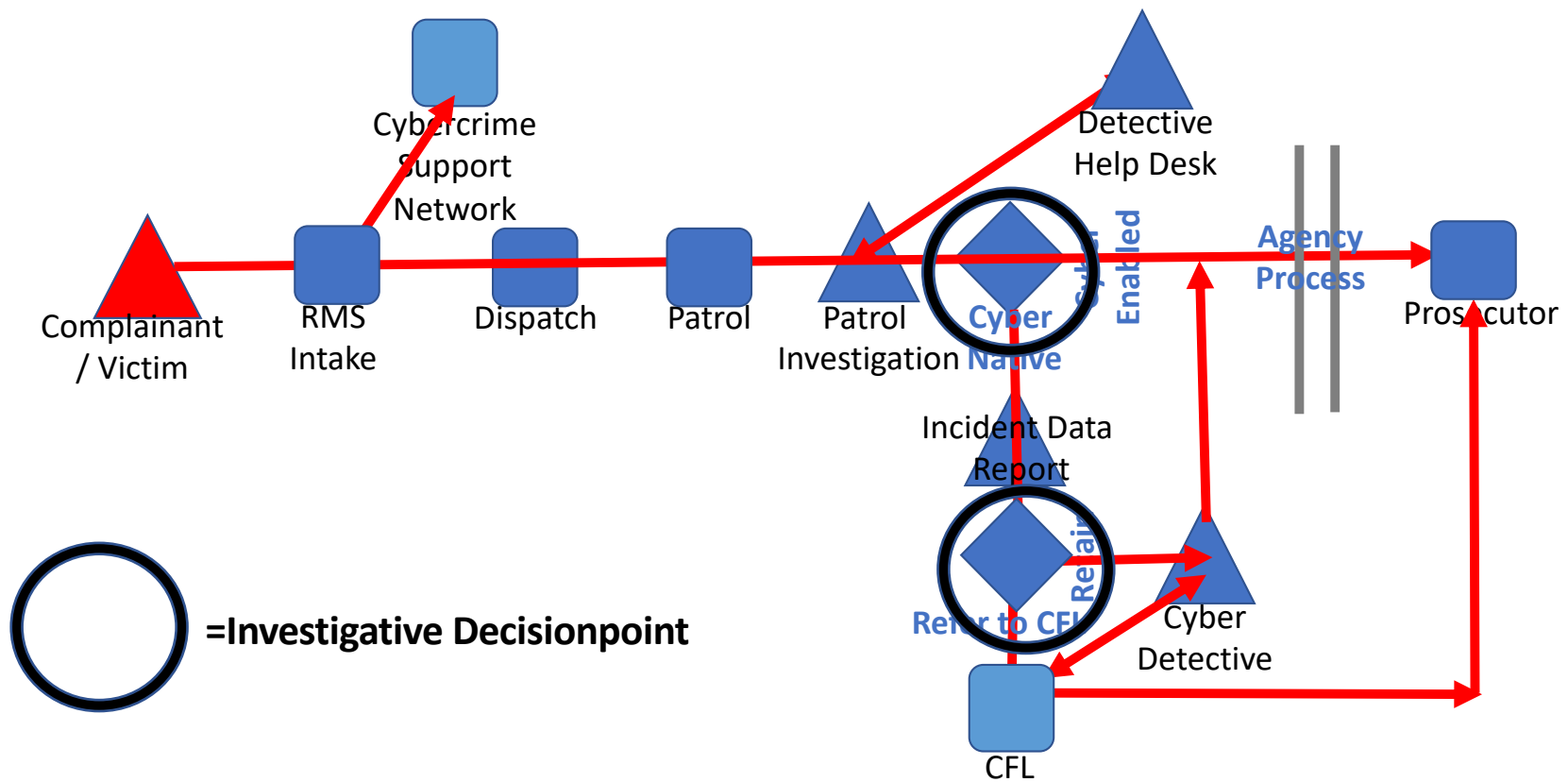
Cyber Enabled Investigations Flow Chart



Cyber Native Investigations Flow Chart



Key Cyber Investigative Decisionpoints



Key Cyber Native Investigative Decisions

Q1: Cyber Enabled Crime OR Cyber Native Crime?

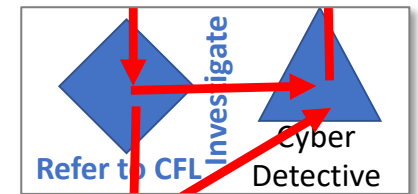
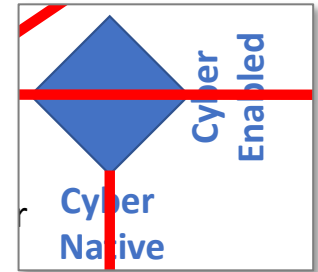
- If Cyber Enabled, nothing new here

If Cyber Native, Complete & Share Cyber Forensic Lab Incident Data Report, & **then decide:**

Q2: Conduct Internal Cyber Detective/ Regional Cyber Task Force Investigation? OR

-Refer to Cyber Forensic Lab, FBI Cyber Task Force, or Other?

- Internal Cyber Detective/Cyber Task Force Investigation requires access to Technical Skills and tools
- BUT NOTE: even if a complete Cyber Investigation is not done, Completing & Sharing CFL Incident Data Report collects law enforcement data useful for many other Investigations



Organize to Respond to Cybercrime Complaints

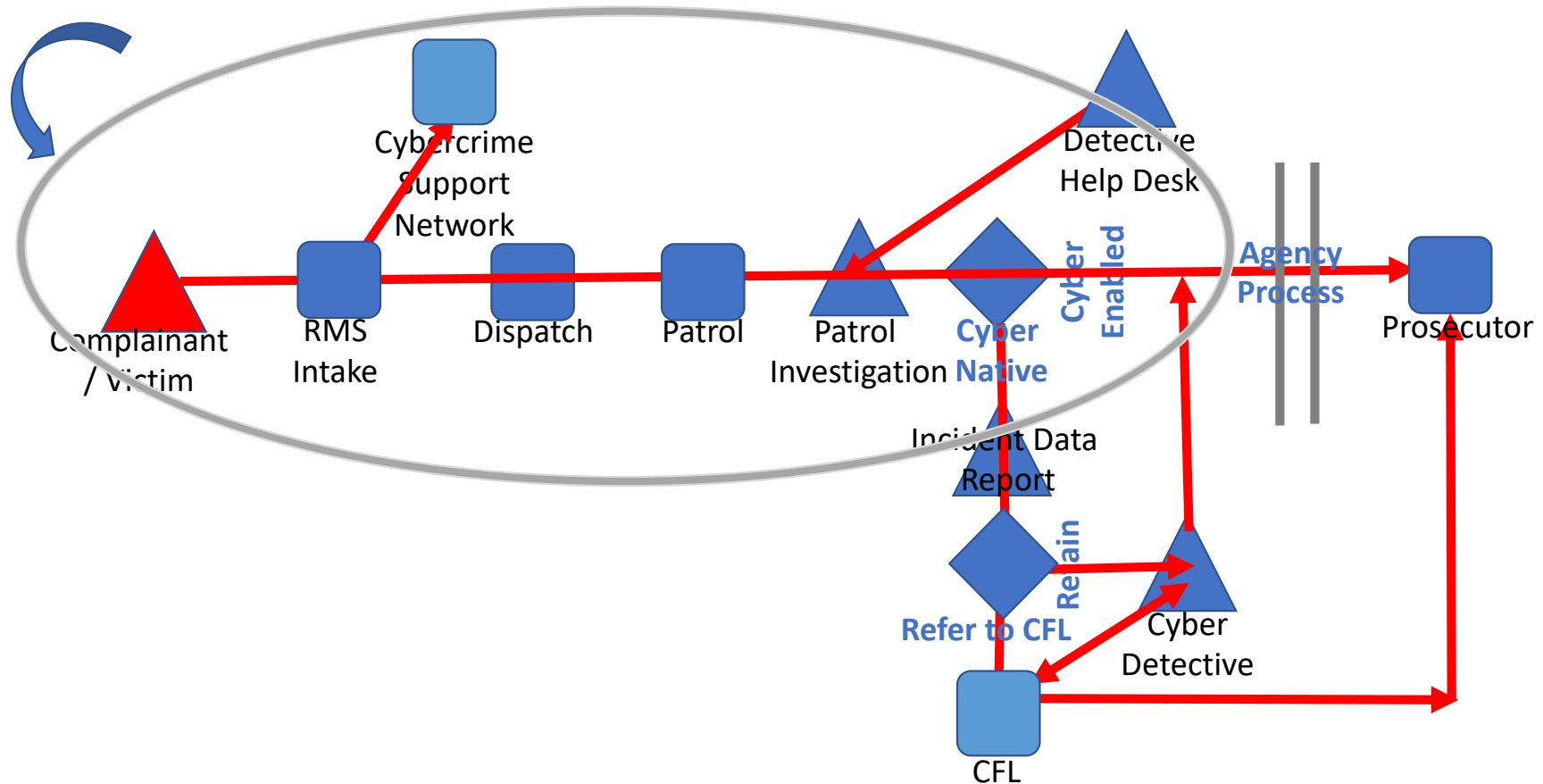
- Consider working with other agencies to form a Regional Cyber Task Force and/or visiting with your State's FBI SAC to assure expert support is available through your SAC's FBI Cyber Task Force
- Consider naming an **Agency Collaboration Officer** responsible for coordination between your Agency and other investigative “partners”

Internally Prepare to Respond to Cybercrime Complaints

Your agency's **Chief of Investigations** or other **Command Staff** implements the following agency roles:

- The agency's **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 **Training Officer** institutes **Cyber Investigation Training** as periodic **Roll Call Training** for all **Patrol** and **other non-technical personnel dealing with the public**, including, in some agencies, **Records Management System (RMS) Intake Personnel**;
- The agency's **Chief of Investigations** designates one or more technically proficient-to-expert cyber investigators as **Cyber Detectives**, who enroll in the **NCIP Forum Information Sharing Environment**;
- Your agency names one or more experienced but **non-Cyber Detectives** to a **"Detective Help Desk"**, to assist front-line investigators think through investigative plans for Cyber Enabled crimes.

Cyber Enabled Investigations



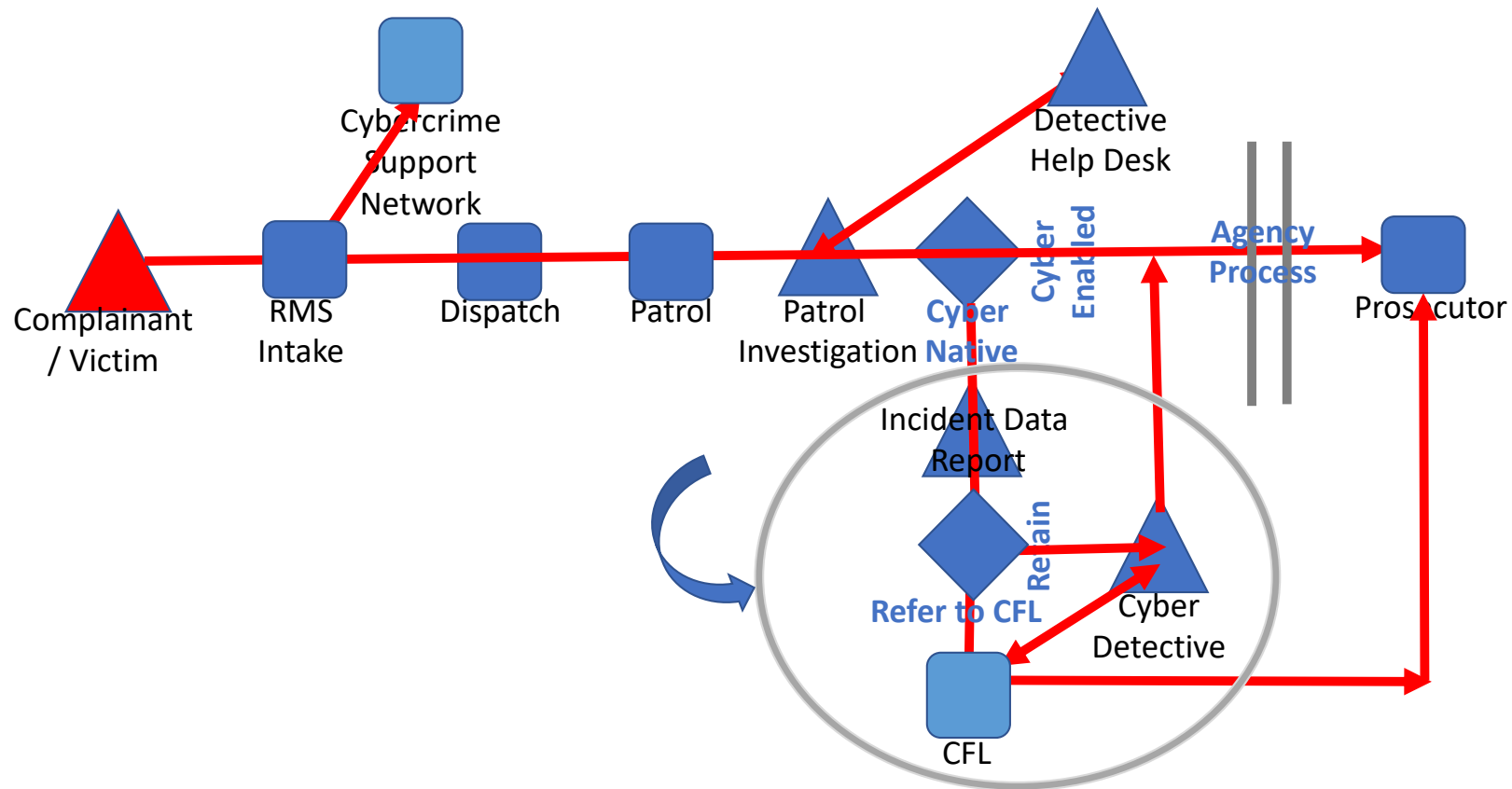
Responding to Cybercrime Complaints

- **PSAP Officers, Dispatch or RMS Intake Personnel:**
 - Refer the **Victim/Complainant** to the **Cybercrime Support Network** for **Cybercrime Victim Services**;
 - Connect the **Victim/Complainant** with **Dispatch** for **Patrol Investigation** by the **Patrol Division**;

Investigating Cyber Enabled Crimes

- The designated **Patrol Investigator**, after determining that the complaint concerns a “**Cyber Enabled**” crime:
 - 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,
 - as in non-cyber cases, reviews the case with an experienced **non-Cyber Detective/Detective Help Desk** to develop an investigative plan for the Cyber Enabled Complaint, to completion of Investigation.

Cyber Native Investigations



Investigating 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** assigned to the case, who works with the Victim/Complainant to complete one of the following: a **CFL Form 1—Forensic Incident Data Report**; a **CFL Form 2—Intrusion Incident Data Report**; or a **CFL Form 3—Digital Media Data Recovery Report**, on the form or, when available, on the **Cyber Native App**;
 - Next, the **Cyber Detective** recommends the Agency either a) Retain and investigate internally (perhaps with support from a Regional Cyber Task Force or FBI Cyber Task Force), or b) Refer to CFL, FBI, or other expert **Cyber Detective**;
 - If the Agency wishes to Refer the case to CFL, the **Cyber Detective** sends the **CFL Incident Data Report** to CFL for an evaluation and quote, and, if agreeable, the investigation proceeds.

As the Prosecution Trial Date Approaches

- **Cyber Detective/Agency/Prosecutor** may seek CFL support for the Prosecution using **CFL Form 4— Prosecution Support Data Report** or, when available, on 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