Defending Digital Campaigns

Cybersecurity Incident Response
Law Enforcement Contacts

The information provided in this document does not, and is not intended to, constitute legal advice. All information and content are for general informational purposes only. Please seek legal advice from your own attorney.

Cybersecurity incidents targeting political campaigns are issues of national concern and election security. **The FBI urges the public and political campaigns to report all instances of potential election crimes to the FBI's local offices, including cybersecurity incidents.**

Any organization that experiences a cybersecurity incident should consider notifying law enforcement. If your campaign suffered a cybersecurity incident, such as hacking or ransomware, it is likely the bad actors are attempting similar attacks on other campaigns. Knowledge of this activity can help law enforcement thwart other attacks and notify others of potential threats.

This document identifies key federal and state law enforcement agencies that handle cybersecurity incidents which may be relevant to campaigns. Agency involvement and jurisdiction is based on a number of factors, such as the nature of the incident, data impacted, and attribution of the incident to a particular group or actor. If you choose to report an incident to Federal law enforcement, in most cases it is advisable to contact the FBI, which can involve other agencies as needed. When an entity experiences a cybersecurity incident, the entity should consult legal counsel and determine whether to contact law enforcement and which agency would best be able to assist with the cybersecurity incident. This document is not intended to represent mandatory reporting requirements.

FEDERAL LAW ENFORCEMENT CONTACTS

Federal law enforcement agencies have advised that if an entity is reporting a cybersecurity incident, the entity should report to only one federal agency for purposes of efficiency and a streamlined response process. The choice of federal agency should be driven by factual, legal and practical considerations.

Federal Bureau of Investigation (FBI)

> **FBI Field Office Cyber Task Forces**: http://www.fbi.gov/contact-us/field
> *Report cybercrime such as computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity*

FBI Guidance:https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view

U.S. Department of Treasury Office of Foreign Assets Control

Office of Foreign Assets Control (OFAC) Sanctions Compliance and Evaluation Division:
Ofac_feedback@treasury.gov
(202) 622-2490
(800) 540-6322
OFAC Licensing Division:
http://licensing.ofac.treas.gov/
(202) 622-2480

Contact OFAC for ransomware incidents that may involve a sanctioned individual or entity.

OFAC Guidance regarding ransomware:
https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

National Cyber Investigative Joint Task Force

NCIJTF CyWatch 24/7 Command Center:
cywatch@ic.fbi.gov
(855) 292-3937
Report cybercrimes and intrusions that require assessment for action, investigation and engagement with local field law offices.

Department of Homeland Security - Cybersecurity and Infrastructure Security

NCCIC:
NCCIC@hq.dhs.gov
(888) 282-0870
United States Computer Emergency Readiness Team:
http://www.us-cert.gov
Report suspected or confirmed cybersecurity incidents, including when affected entity may be interested in government assistance in removing the threat actor, restoring operations, and recommending ways to further improve security

United States Secret Service – Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):

http://www.secretservice.gov/contact/field-offices
http://www.secretservice.gov/ectf.shtml
Report cybercrime, such as transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.

CISA Incident Reporting Guidance:
https://www.cisa.gov/sites/default/files/publications/Law%20Enforcement%20Cyber%20Incident%20Reporting.pdf

Internet Crime Complaint Center (IC3)

Internet Crime Complaint Center (IC3): http://www.ic3.gov
Report individual instances of cybercrime online, which will be distributed to appropriate agencies

STATE LAW ENFORCEMENT CONTACTS

The following chart lists resources for state law enforcement and other state government agencies responsible for handling cybersecurity incidents. In addition to the state agencies below, entities can also report to local law enforcement, such as local police departments. Although many states also have consumer protection divisions that assist consumers with identity theft issues, this chart does not include such divisions solely dedicated to consumer protection.

Note that entities may be required to report certain data breaches to designated state regulators. Please see State Data Breach Notification Laws Chart for more details.

STATE	AGENCY
Alabama	CyberCrimes Unit, State of Alabama Law Enforcement Agency https://www.iacpcybercenter.org/labs/alabama-law-enforcement-agency-cybercrimes-unit/
Alaska	Alaska Department of Public Safety, Technical Crimes Unit https://dps.alaska.gov/ast/abi/technicalcrimes
Arizona	Criminal Investigations Division, Arizona Department of Public Safety https://www.azdps.gov/organization/cid
	Data Privacy and Security, Arizona Attorney General https://azag.gov/consumer/data-breach
Arkansas	Special Investigations Division, Arkansas Attorney General https://www.arkansasag.gov/arkansas-lawyer/special-investigations-division/
California	California Cyber Crime Center, State of California, Department of Justice https://oag.ca.gov/cyberexploitation
	eCrime Unit, State of California, Department of Justice

	https://oag.ca.gov/ecrime
	Bureau of Investigation, State of California, Department of Justice https://oag.ca.gov/bi
Colorado	Identity Theft, Fraud and Cyber Crimes Unit, Colorado Bureau of Investigations https://colorado.gov/pacific/cbi/identity-theftfraud-and-cyber-crimes-unit-contacts
Connecticut	The District of Connecticut's Cybercrime Program, U.S. Department of Justice https://justice.gov/usao-ct/cybercrime-program
	Computer Crimes / Electronic Evidence Laboratory, Dept. of Emergency Services / Public Protection http://ct.gov/despp/cwp/view.asp?a=4154&q=487836
Delaware	Delaware State Police Intelligence Unit http://dsp.delaware.gov/intelligence_unit.shtml
Florida	Computer Crime Center, Florida Department of Law Enforcement https://www.fdle.state.fl.us/FCCC/FC3-Home.aspx
Georgia	Georgia Bureau of Investigation, Cyber Crime Center (G3C) https://investigative-gbi.georgia.gov/specialized-units/georgia-cyber-crime-center-g3c
Hawaii	Crime Prevention and Justice Assistance Division https://ag.hawaii.gov/cpja/ccp/internetsafety/if-you-need-help-document/
Idaho	Cyber Crime Unit, Idaho State Police https://isp.idaho.gov/cybercrime/
Illinois	Illinois Attorney General, Illinois Computer Crime Institute http://illinoisattorneygeneral.gov/communities/hitech/icci.html
Indiana	Cybercrime & Investigative Technologies Section, Indiana State Police http://in.gov/isp/3234.htm
	Indiana State Police Cyber Crime Unit http://iacpcybercenter.org/labs/indiana-state-police-cyber-crime-unit-crimes-against-children-unit/
	Report an Internet Crime, Indiana State Police http://in.gov/isp/2461.htm
Iowa	Iowa Information Security Division https://iso.iowa.gov/how-report-incident
Kansas	Cyberstalking, Kansas Attorney General https://ag.ks.gov/public-safety/internet-safety/internet-safety-for-parents/cyberstalking
Kentucky	Cyber Safety, Kentucky Attorney General https://ag.ky.gov/Priorities/Protecting-Kentuckians/Pages/cyber-safety.aspx
Louisiana	The Cyber Crime Unit, Louisiana Department of Justice, Attorney General https://www.ag.state.la.us/Article/41

Maine	Computer Crimes Unit, Maine State Police https://maine.gov/dps/msp/investigation-traffic/computer-crimes-unit
Maryland	Computer Crimes Unit, Criminal Enforcement Division, Maryland State Police http://mdsp.maryland.gov/Organization/Pages/CriminalInvestigationBureau/CriminalEnforcementDivision.aspx
Massachusetts	The Cyber Crime Division, Office of the Attorney General http://mass.gov/ago/bureaus/criminal/emcc/the-cyber-crime-division/
Michigan	Michigan State Police, Cyber Section http://michigan.gov/msp/0,4643,7-123-72297_72370_72379---,00.html
	State of Michigan, Reporting Cyber Crime http://michigan.gov/som/0,4669,7-192-78403_78404---,00.html
Minnesota	Minnesota Financial Crimes Task Force https://dps.mn.gov/divisions/bca/bca-divisions/investigations/Pages/mn-financial-crimes-task-force.aspx
Mississippi	Cyber Crime Unit, Mississippi Attorney General http://ago.state.ms.us/divisions/cyber-crime/
Missouri	Digital Forensics Investigative Unit, Missouri State Highway Patrol http://mshp.dps.missouri.gov/MSHPWeb/PatrolDivisions/DDCC/Units/ComputerForensicUnit/index.html
Montana	Computer Crime, Montana Department of Justice https://dojmt.gov/enforcement/investigations-bureau/computer-crime/
	Investigations Bureau, Montana Department of Justice https://dojmt.gov/enforcement/investigations-bureau/
Nebraska	Nebraska State Patrol, Investigative Services https://statepatrol.nebraska.gov/divisions/investigative-services
Nevada	Nevada Cyber Crime Task Force https://ag.nv.gov/Hot_Topics/Victims/Victim/
New Hampshire	New Hampshire Criminal Justice Bureau https://doj.nh.gov/criminal/
	Major Crime Unit, Investigative Services Bureau, New Hampshire Department of Safety https://nh.gov/safety/divisions/nhsp/isb/majorcrime/index.html
New Jersey	Cyber Crimes Unit, New Jersey State Police http://njsp.org/division/investigations/cyber-crimes.shtml
	High Tech Crime Bureau, New Jersey State Police http://njsp.org/division/investigations/high-tech-crime.shtml
	Digital Technology Investigations Unit, New Jersey State Police http://njsp.org/division/investigations/digital-tech-investigations.shtml
	The Official Website for the State of New Jersey, Internet Safety http://state.nj.us/nj/safety/internet/
New Mexico	New Mexico State Police, Criminal Investigation Section https://nmsupolice.com/criminal-investigations-section/
New York	Computer Crime Unit, New York State Police

	https://troopers.ny.gov/Criminal_Investigation/Computer_Crimes/
	Bureau of Internet and Technology, New York State Attorney General's Office https://ag.ny.gov/bureau/internet-bureau
	The New York County District Attorney's Office, Resources for Victims of Identity Theft/Cybercrime http://manhattanda.org/resources-victims-identity-theftcybercrime
North Carolina	North Carolina State Bureau of Investigation http://ncsbi.gov/
North Dakota	North Dakota State and Local Intelligence Center https://www.ndslic.nd.gov/cyber-program
Ohio	Cyber Crimes Unit, Bureau of Criminal Investigation, Ohio Attorney General http://www.ohioattorneygeneral.gov/Law-Enforcement/Bureau-of-Criminal-Investigation/Investigation-Division
Oklahoma	Computer Crimes Unit, Oklahoma State Bureau of Investigation https://ok.gov/osbi/Investigative/Computer_Crime_Unit/index.html
Oregon	Criminal Justice, Oregon Department of Justice https://doj.state.or.us/oregon-department-of-justice/divisions/criminal-justice/
Pennsylvania	Internet Crimes Investigation, Pennsylvania State Police https://www.psp.pa.gov/law-enforcement-services/Pages/Training%20Courses/INTERNET-CRIMES-INVESTIGATION.aspx
Rhode Island	Computer Crimes Unit, Rhode Island State Police http://risp.ri.gov/ccu/
South Carolina	Computer Crimes Center, South Carolina Law Enforcement Division https://www.sled.sc.gov/computercrimes.html
South Dakota	South Dakota Cybersecurity Group https://cybersecurity.sd.gov/default.aspx
Tennessee	Cybercrime, Tennessee Bureau of Investigation https://tn.gov/tbi/crime-issues/crime-issues/cybercrime.html
	Identity Crimes Unit, Tennessee Department of Safety & Homeland Security https://tn.gov/safety/news/2014/3/25/tennessee-department-of-safety-homeland-securitys-identity-crimes-unit-to-h.html
Texas	Computer Information Technology and Electronic Crime, Texas Department of Public Safety https://www.dps.texas.gov/CriminalInvestigations/citecUnit.htm
Utah	Cyber Crimes, State Bureau of Investigation, Utah Department of Public Safety https://sbi.utah.gov/cyber-crimes/
Vermont	Technology Investigation Unit, Vermont State Police https://vsp.vermont.gov/criminal/technology
	Vermont Intelligence Center, Vermont State Police http://vsp.vermont.gov/criminal/vic

Virginia	Computer Crime, Attorney General of Virginia https://www.oag.state.va.us/ccsweb2/
	High Tech Crimes, Virginia State Police https://pshs.virginia.gov/homeland-security/cyber-security/
Washington	Internet Crime, Washington State Attorney General http://atg.wa.gov/internet-crime
	Access Washington, Internet Crime https://access.wa.gov/topics/consumerprotection/technology/internetcrime.html
West Virginia	West Virginia Office of Technology https://technology.wv.gov/security/Pages/default.aspx
Wisconsin	Division of Criminal Investigation, Wisconsin Department of Justice https://www.doj.state.wi.us/dci/division-criminal-investigation-dci
Wyoming	Computer and High Tech Crimes, Wyoming Division of Criminal Investigation http://wyomingdci.wyo.gov/dci-operations-section/computer-and-high-tech-crimes