utah govops

UTAH DEPARTMENT OF GOVERNMENT OPERATIONS

# Utah Cyber Center - City & County Outreach Program

**Local Governments**
**November 2023**

# Agenda

- What is the Utah Cyber Center?
- City and County Outreach Program
- Projects and Services Available
- Incident Response Plans and Resources
- Information Sharing and Analysis Centers
- Reporting System Security Breaches
- Migrating to a Top Level Domain

# What is the Utah Cyber Center?


## Utah Cyber Center

**Director: Philip Bates, State CISO**

- Cybersecurity Commission
- Federal Bureau of Investigation
- Utah Office of the Attorney General

- Department of Public Safety
  - State Bureau of Investigation
  - Division of Emergency Management
  - Statewide Information and Analysis Center
- Division of Technology Services
  - Enterprise Security Services
  - City/County Outreach

- Utah Education and Telehealth Network
- CISA
- ULCT & UAC

# What is the Purpose of the UCC?

## What are the duties of the Utah Cyber Center?

- By June 30, 2024 develop a statewide strategic cybersecurity plan for executive branch agencies and other governmental entities.
- Incorporate the Enterprise Security Services into the Cyber Center, and through their efforts continue to provide cybersecurity services to the executive branch.
- At the request of a governmental entity, coordinate/assist cybersecurity incident breach response.

# What is the Purpose of the UCC?

## What are the duties of the Utah Cyber Center?

- Promote cybersecurity best practices.
- Share cyber threat intelligence.
- Receive reports of breaches of system security.
- Coordinate cybersecurity response efforts between state, local, and federal entities.
- Support the development cybersecurity professionals through partnerships with local institutions of higher education.

utah govops

UTAH DEPARTMENT OF GOVERNMENT OPERATIONS

# Utah Cyber Center City and County Outreach Program

# City & County Outreach Program

- Our primary mission is to assist local government entities in their efforts to securely provide IT services to their communities.
- To support our mission we provide the following services to local governments:
  - Assist in Incident Response
  - Facilitate Training
    - Both technical training for security professionals, as well as general employee security awareness training
  - Assist in Securing Funding
    - Grants, State funding, Hardware Donation
    - Promote the use of Shared State Contracts - Leveraging the purchasing power of the State

# UCC Outreach - Year One Priorities

- Assess the general cybersecurity posture across the state to identify gaps and needs through partnered research programs.
- Develop a Whole-of-State Cybersecurity Model with managed or shared services.
- Support the Mission of the UCC by assisting in the development a web presence to facilitate reporting and information sharing.
    - **cybercenter.utah.gov**
- Seek sustained funding methods to be built locally by State and Local entities as well as securing funds available through Federal Grant programs.

utah govops

UTAH DEPARTMENT OF GOVERNMENT OPERATIONS

# City and County Outreach - Current Programs

# Current Programs

- Using the information gathered from our partnered research and evaluation of the maturity baseline the following projects have been approved for cities, counties and select special districts:
  - Endpoint Protection services through an MDR implementation which will provide advanced security measures and be supported by a team of expert security analysts 24x7.
  - Vulnerability Management services to help identify vulnerabilities on computers and servers.
  - A robust security awareness training platform to help educate government employees.
  - Training and exam vouchers for local government Information Technology staff through CompTIA, SANS, EC-Council and others.

# How Do You Sign Up?

- Fill out the “Utah Cyber Center Form” (QR code) identifying which services your organization would like to participate in.
- Basic information such as your entity name, type, contact name, job title, email and phone number along with the specific services your organization is interested in.
- Our team will be in contact with you.

# UCC Outreach - What's Next?

- Over the next year, our team will continue to help support and improve the duties as discussed previously.
- Identify next steps or projects to help reduce risk and build up cyber resilience.
- Continue to build relationships and trust with the local government.

utah govops

UTAH DEPARTMENT OF GOVERNMENT OPERATIONS

# Incident Response

# Incident vs Breach

Incident

- An event or occurrence that may compromise the security or integrity of an organization's information systems or data.
- Incidents can range from minor issues, such as an employee clicking on a suspicious link, to major disruptions like a server outage.

Breach

- A specific type of incident that involves the unauthorized access, disclosure, or acquisition of sensitive or confidential information.
- Breaches are often the result of malicious actions, such as hacking or data theft, but can also occur due to accident exposure of data.

- Incidents leading to breaches can have serious legal, financial, and reputational consequences.

# Incident Response Plans

- An incident response plan can help outline who to contact in the event of a breach and how to respond quickly to reduce the impact to an organization.
- Incident response plans can take time, effort, and coordination to put in place - but well worth it.
- The Utah Cyber Center has put together a list of resources your organization can use to help plan and create your own incident response plan.

# Incident Response Plan Resources

- **Cybersecurity Incident Response Guide (MS-ISAC)** - Very easy to follow guide for preparing and building and incident response plan. *We recommend starting here*.
- **Incident Response Plan Basics** - Provides a very high level view of what you should do before, during, and after and incident.
- **Cybersecurity Incident & Vulnerability Response Playbooks** - Provides a good response framework to follow but in particular provides checklists, that after adapted, can be helpful during an incident.
- **Incident Response Standard** - Provides a Policy Template that you can follow.
- **NIST Computer Incident Handling Guide** - If you are to this level, it provides the most comprehensive guide of how to build an incident response policy, plan, and everything that needs to be included.

# Incident Response - What We Can Do to Assist

The Utah Cyber Center can provide governmental entities with assistance in responding to a breach of system security, which may include:

- Conducting all or part of the investigation
- Assisting law enforcement with the investigation if needed
- Determining the scope of the breach of system security
- Assisting the governmental entity in restoring the reasonable integrity of the system
- Providing any other assistance in response to the reported breach of system security

utah govops

UTAH DEPARTMENT OF GOVERNMENT OPERATIONS

# Information Sharing and Analysis Centers (ISACs)

# National ISACs

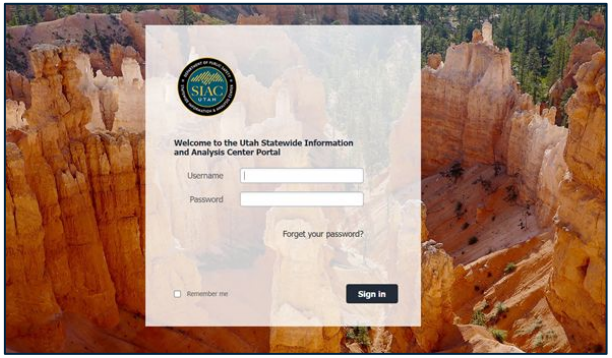
- ISACs help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards.
- They help disseminate actionable threat information to their members and often provide their members with tools to mitigate risks and enhance resiliency.
- Examples of ISACs: Emergency Management and Response ISAC, Health ISAC.
- For a full list of member ISACs, please visit: https://www.nationalisacs.org/member-isacs-3

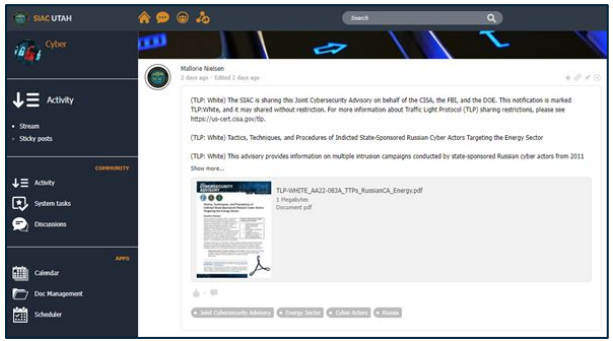
MS-ISAC®
Multi-State Information Sharing & Analysis Center®

WATER ISAC

utah govops

# Utah SIAC Intelligence Portal




- The Utah SIAC Intelligence Portal provides a single, secure, CJIS-compliant location for members to retrieve and consume intelligence information.
- SIACintel.utah.gov provides category specific, finished intelligence.
    - All members are vetted and must have a need-to-know in order to join certain communities of interest. Current communities of interest include communities for law enforcement, Cyber, Elections, and the Private Sector, Government, and Critical Infrastructure community.
    - Contact the SIAC via SIAC@Utah.gov to request an account.
        - Include your professional title & organization name

utah govops

UTAH DEPARTMENT OF GOVERNMENT OPERATIONS

# Security Breach Reporting

# Security Breach Reporting - What is a Breach of System Security?

UC 13-44-102. Definitions.

- "Breach of system security" means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.

# Security Breach Reporting
# UC 13-44-202

*Effective 5/3/2023*

**13-44-202. Personal information -- Disclosure of system security breach.**

(1) (a) A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.

(b) If an investigation under Subsection (1)(a) reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.

# Security Breach Reporting - Requirements

UC 13-44-202

- (1)(c) Personal information relating to **500 or more** Utah residents:
  - Report to the Utah Office of the Attorney General and the Utah Cyber Center
- (1)(d) Personal information relating to **1000 or more** Utah residents
  - Report to AG, UCC & notification to each consumer reporting agency

# Security Breach Reporting - When to Report?

UC 13-44-202

- (2) Required to provide notification in the “most expedient time possible without reasonable delay”
  - (a) considering legitimate investigative needs of law enforcement, as provided in Subsection (4)(a)
  - (b) after determining the scope of the breach of system security; and
  - (c ) after restoring the reasonable integrity of the system.

# Security Breach Reporting - Confidentiality and Disclosure

UC 13-44-202

- (6)(a) Records submitted to AG and UCC and information produced, or any coordination and assistance provided are presumed confidential and are a protected record if a written claim of business confidentiality and a concise statement of reasons supporting the claim of business confidentiality (63G-2-309).
- (6)(b) Disclosure of information provided under (1)(c) or produced in (6)(a) may only occur if:
  - Disclosure is necessary to prevent imminent and substantial harm; or
  - Information is anonymised

# Where Do You Report a Breach of System Security?

cybercenter.utah.gov

# Utah Cyber Center

The Utah Cyber Center was created to coordinate efforts between State, Local, and Federal resources to bolster statewide security and help defend against future cyber attacks, by sharing cyber threat intelligence, best practices, and through strategic partnerships.

## Our Duties

The Utah Cyber Center's duties are defined in Utah State Code 63A-16-510. Some of these duties include the creation of a Statewide Strategic Cybersecurity Plan, receiving reports of breaches of system security as outlined in Utah Code 13-44-202 and 63A-16-511, and identifying sources of funding to make cybersecurity improvements throughout the state.

Additionally, the Utah Cyber Center is also tasked with developing incident response plans for the coordination of local, state, federal, and private sector breaches. At the request of local governments, the Utah Cyber Center will also assist in coordinating an incident response for breaches.

The final duty of the Utah Cyber Center is to develop a sharing platform to provide cybersecurity information, recommendations, and best practices, and threat intelligence

## Need to Report a Breach?

In 2023 Utah Legislature passed S.B. 127 Cybersecurity Amendments which created reporting requirements for breaches related to Utah resident information. Details for these requirements can be found in Utah codes 13-44-202 and 63A-16-511.

### Additional Reporting Requirements

Depending on the type of data involved in the breach, you may be subject to additional reporting requirements. Please use the links below to find out more information about the different types of data.

- Personal Health Information (HIPAA)
- Federal Tax Information (FTI)
- Criminal Justice Information (CJIS)
- Payment Card Information (PCI-DSS)

## Breach Reporting Form

### Submitter Details

**Submitter Name** *

**Submitter Email** *

**Submitter Phone** *

Provide a telephone number

**Are you making notification on behalf of another entity?** *

No Yes

**Has legal counsel been retained?** *

No Yes

## Affected Entity Details

**Affected Entity Name** *

**Affected Entity Business Address** *

**Type of Entity** *

Select or search options

## Incident Information

**Summarized description of the breach** *

**Total number of individuals affected** *

**Number of affected Utah residents** *

**When did the breach occur?** *

M/D/YYYY h:mm A

**When was the breach discovered?** *

M/D/YYYY h:mm A

**Type of Breach** *

Select or search options

**Data involved in breach** *

Select or search options

**Please provide any additional details**

## Notifications

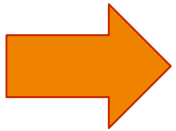
**Were the impacted individuals notified?** *

No Yes

**Has this breach been reported to other entities?** *

No Yes

**Additional comments**



Submit

**Data Use Disclosure:** The information on this form is being collected pursuant to the disclosure and reporting requirements of the Utah Protection of Personal Information Act (UPPIA), in particular Utah Code § 13-44-202. It will be used for the purposes set forth in the UPPIA, potentially including enforcement pursuant to Utah Code § 13-44-301. All information provided on this form is presumptively classified as "public" in accordance with the Utah Government Records Access and Management Act (GRAMA), Utah Code Section 63G-2-301. Confidential information should not be included on this form. If such information needs to be submitted, please indicate that such additional information is available and identify the person who should be contacted regarding such information. Confidential information should only be provided in accordance with the provisions of the UPPIA that provide protection for such information, including Utah Code § 13-44-202(6) and/or § 13-44-301(7).

# How Will Reporting Help?

The Utah Cyber Center would like to use any indicators of compromise (IOCs) to help protect others in the event of a system breach.

IOCs provide valuable information on systems that have been compromised and can then be used to help others who may be in a similar vulnerable situation. IOC examples can include information such as IP addresses, domain names, email addresses, file names, etc.

When reporting a breach, make sure to include as much information as possible with tactics, techniques, and procedures on how the incident occurred within your organization.


# Authorized Top Level Domain

# Use of an Authorized Top Level Domain

***UC 63D-2-105***

Beginning **January 1, 2025** all governmental entities within the state of Utah must use an authorized top level domain for their website address and the email addresses used by the entity and its employees.

# What is an Authorized Top Level Domain?

- A top-level domain (TLD) is the part of an email or website's address that comes after the "dot".

  johndoe@utah-city.gov

  www.utah-city.gov

- Helps classify websites on the internet.
- TLDs will vary depending on the type of entity. However, the three authorized top level domains are **.gov**, **.edu**, and **.mil**.

# Are There Any Exceptions?

A governmental entity may operate a website that uses a non-authorized top level domain if it is clear that the site is not the primary site of the entity and one of the following is true:

- The site is solely for internal use and not intended for members of the public;
- The site is temporary and in use for less than one year;
- The site is related to an event, program, or informational campaign operated in partnership with a non-governmental organization.

# Is It Possible to Obtain an Exemption?

It is possible to request an exemption from the requirement if there are **extraordinary circumstances** under which the use of an authorized top level domain would cause demonstrable harm to citizens or businesses and the executive director or chief executive of the governmental entity submits a written request to the Chief Information Officer of the State of Utah.

Contact the Utah Cyber Center regarding your exemption request.

# How Do You Register for a .gov Domain?

To register and receive a .gov domain, visit get.gov/registration. CISA manages the .gov domain and can be contacted directly for assistance.

- Phone: 1-877-734-4688
- Email: registrar@dotgov.gov
- FAQs can be viewed at get.gov/help

*Requests for new .gov domains are paused until January 2024

Subdomains

Eligible governmental entities within the state of Utah can register a subdomain on the **utah.gov** domain.

# What are the Benefits of Using an Authorized Top Level Domain?

Using an authorized top level domain **bolsters the confidence and legitimacy** to the people interacting with a governmental entity through the web. These domains are strictly controlled and only authorized and vetted entities can obtain domain registration on these platforms.

The .gov top level domain and utah.gov subdomain is free of charge to qualifying entities.

# Thank You!

For questions or comments:
✉️ cybercenter@utah.gov

Or visit our webpage:
🌐 **cybercenter.utah.gov**