MS-ISAC®

Intel Paper

# WHOIS Changes Likely to Affect SLTT Governments

May 9, 2018 – IP2018-0521

On May 25, 2018, it is highly likely that the Internet Corporation for Assigned Names and Numbers (ICANN) will greatly restrict public WHOIS information while it creates and implements a plan to become compliant with European Union (E.U.) Regulation 2016/679 General Data Protection Regulation (GDPR). This change will almost certainly impact many state, local, tribal, and territorial (SLTT) governments that rely on WHOIS data.

**What is WHOIS?** WHOIS is a service that allows the public to query information about a domain registrant. This type of information often includes the name, address, IP address, and contact information for the registrant. Information from WHOIS is useful in identifying the owners of domains, which can be useful for determining whether or not a domain is legitimate, what other domains are owned by the same registrant or are related, and identifying contact information if it is necessary to reach the domain owner.

**What is the GDPR?** The GDPR is a regulation governing the privacy of EU data subjects and affects all organizations collecting, processing, and/or storing EU citizens' and residents' data, including names, addresses, IP addresses, and any other identifying information. The legislation has international reach, governing any EU data subjects, regardless of where that person resides or the data is stored. Entities that do business within the EU, including ICANN, will almost certainly have repercussions for non-compliance.

It is highly likely that WHOIS information will be redacted indefinitely until a GDPR compliant system is implemented, because the WHOIS system collects and displays names, emails, and other contact information from registrants that must be protected under the GDPR.

- ICANN announced it would not take legal action against registrars for noncompliance relating to the handling of registration data until it creates a new WHOIS data agreement that takes GDPR into account. This announcement has resulted in some domain registrars redacting registrant contact information from the WHOIS service.
- ICANN has proposed a solution that will be GDPR compliant, but has assessed that a GDPR compliant system will likely take until December 2018, or later, to develop and implement. Elements of the proposed solution include limiting access to WHOIS data to verified authorities with a need-to-know.
- The Article 29 Data Protection Working Party (WP29), which will be responsible for enforcement under the GDPR, assessed that ICANN's proposed interim model is not sufficient for GDPR compliance, potentially extending the rollout time for the interim solution and making it more likely that WHOIS data will not be publicly available after May 25.
- WP29 has rejected ICANN's requests for a moratorium on GDPR enforcement while the organization works to implement a GDPR compliant system.

It is likely that many SLTT governments will find some tasks, such as phishing email and malware analysis, spoofed domain monitoring, domain blacklisting, and law enforcement activities more difficult as a result of the loss of WHOIS information. Many SLTT governments use WHOIS information in their day-to-day operations do so by either utilizing third-party services or by querying the service directly.

- SLTT governments likely use WHOIS queries in *daily cybersecurity operations* to analyze malware and phishing messages, assess the legitimacy of websites, identify fraud, and issue takedown and abuse requests.
- Affected *third-party services* that will possibly impact SLTT governments potentially include cybersecurity service providers and threat intelligence platforms that use WHOIS data to alert customers of domain spoofing, identify related domains, create blacklists, and discern relationships between registrants and infrastructure.
- Furthermore, many SLTT *law enforcement activities* are likely to be negatively impacted as law enforcement officers often use WHOIS data to identify evidence regarding malicious actors and actions, assess threat location and jurisdiction, serve legal orders, and as evidence in legal proceedings.

**RECOMMENDATIONS:**

Due to the forthcoming changes and potential unavailability of WHOIS information, the MS-ISAC recommends that SLTT governments identify where WHOIS data is being used and by whom. The following questions and research points will aid in determining the potential impact to your organization:

- Do you perform WHOIS queries as part of your daily duties? If yes, how do you use these services? In addition to information technology (IT) and cybersecurity staff, it may be useful to ask this question of anyone with an investigatory role, including law enforcement, fire department and fraud investigators, licensing departments, legal counsel, and teachers who may use WHOIS as part of classwork.
- Do any third party services use or potentially use WHOIS information, such as a spam mitigation service, forensics or malware analysis service, or threat intelligence platform? If so, have they issued a statement regarding the potential impact and will they continue to meet your needs?
- If you run a proxy service or log outbound web traffic, query the files for traffic to known WHOIS resources or websites that can indicate additional WHOIS users. Such websites would include ICANN.org and known WHOIS providers and domain registrars.

TLP: WHITE The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information, as well as 24x7 cybersecurity assistance for SLTT governments, is available by contacting the MS-ISAC at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/.