User Story:

	User Type	Data Elements	Purpose Specification
1	As a [Insert User Type from list]	I use the following data elements: [insert from list, add anything missing]	For the purpose of [specify]
2	Law Enforcement Authority	I frequently use data elements from WHOIS including but not limited to names, contact information, creation date, etc.	Helping identify possible suspects and victims, as well as trying to help locate relevant evidence and appropriate witnesses/custodians
3	Law Enforcement Authority	WHOIS is used on a regular basis with almost every cybercrime / IP investigation to identify the domains, IP addresses, registrants, (countries), etc.	- To aid in the investigation by identifying the subjects of the investigation (or the victims) - To identify the proper ISP, webhosting company, or domain registrar to subpoena subscriber and transactional information - To use in search warrant affidavits for to support the probable cause - To use in court orders as part of the basis for the order - To use the results in trial as an exhibit (as a printout or screen shot sponsored by the agent)
4	Law Enforcement Authority	WHOIS	As an investigation develops and new IP addresses are discovered, WHOIS enables us to quickly determine where to serve process to find additional relevant information.

5	Law Enforcement Authority	In international investigations, I routinely look up IP addresses in WhoIs to identify the specific service provider in formulating MLAT requests to Italy.	For the purpose of providing the most detailed information possible about the ultimate source of the information we are seeking (including the address of the service provider) in order to facilitate and expedite our requests through the foreign justice system.
6	Law Enforcement Authority	We use multiple elements from WHOIS lookups as an important first step in cybercrime investigations, and other criminal investigations to identify leads and critical next steps to advance the investigation. The important elements from WHOIS lookups include, among other things, the IP address. the registrant name and contact e-mail address, and ISP abuse contact information.	Quickly determining the IP address and ISP belonging to malicious criminal infrastructure allows us to quickly take steps to preserve and issue legal process to obtain critical data. This can include quick outreach to other member nations that are part of the Budapest Convention on Cybercrime for preservation through the 24/7 Network, and outreach to foreign law enforcement partners to coordinate responses to common cybercrime threats that broadly impact security. That information allows us to find connections with other investigations that involved malicious imputer network infrastructure associated with the registrant, and issue legal

			process to obtain information as to payment for the computer network infrastructure, which can in turn assist with further identification of malicious networks that we can not only use to advance criminal investigations, but provide to victims to help protect their systems from ongoing criminal conduct.
7	Law Enforcement Authority	I use the following data elements: ICANN WHOIS	For the purpose of discovering who operates a given domain and how I can communicate with and/or serve legal process on them in the form of subpoenas and search warrants.
8	Law Enforcement Authority	I use all of the WHOIS information	To develop investigative leads.
9	Law Enforcement Authority	I use the following data elements: creation date, renewal date, and registrant's email address associated with a domain name	For the purpose of identifying accounts to search pursuant to search warrants, if we believe the website or domain is being used to facilitate a crime. The dates establish the time period to search, and renewal dates are helpful to freshen staleness issues.
10	Law Enforcement Authority	I use all elements of WHOIS	As a first step in nearly every cyber-crime criminal investigation in order to identify leads
11	Law Enforcement Authority	All elements	I use WHOIS on a daily basis. If I get a preservation request from one of our colleagues that does not have all the required provider information, I use WHOIS to quickly get that information so the request can be processed in a timely manner. Oftentimes, the requests are urgent and having this tool to help expedite the request is essential for performing my job.

12	Law Enforcement Authority	All data elements are used	The use of WHOIS has facilitated several international investigations, which have allowed US prosecutors to share leads with foreign colleagues, leading both to extraditions to the US as well as investigations by our overseas partners. This international cooperation—especially in cyber and terrorism matters—would be hampered without the WHOIS lookup tool, as would the entire 24/7 Preservation system established by the Budapest Convention.
13	Law Enforcement Authority	I have used WHOIS information (including registrant and organization name, mailing address, and creation and update dates) in many of my criminal investigations.	I have used WHOIS to develop leads; help assess the likelihood of U.S. jurisdiction; assist in verifying actors' identity; determine whether domestic tools can be used to seek additional information or whether a foreign request for evidence will be necessary (and determine, given the country, whether such a foreign request would likely be successful)
14	Law Enforcement Authority	All data elements are critically used.	It's the first step in most cases involving electronic information.
15	Law Enforcement Authority	We use WHOIS as a first step in nearly every criminal investigation in order to identify leads	When our agency receives a request, for access to software or documents , the person(s) responsible for reviewing those requests can make quick and time saving judgments (of disqualification), if the request comes from someone claiming, for example, to be a US-based University professor, but using an IP address leased out of another country. And they can only do this if they have access to WHOIS resources and can lookup IP addresses.

16	Law Enforcement Authority	I personally use WHOIS lookups about as often as I use Google searches in my investigations. It is an essential part of my training and outreach with local law enforcement	In a major fraud investigation, WHOIS lookups were critical to identifying conspirators responsible for registering fraudulent domains. We also have had several groups of individuals using Internet services to lure victims to robberies. Using a WHOIS lookup is critical to quickly aid us in finding the locations where these defendants are operating from, and have led to subpoenas and eventually to search warrants.
17	Law Enforcement Authority	I use the following data elements: Domain and network registrant name and administrative contact.	In order to serve legal process for subscriber information, transactional data, and content of associated server.
	Law Enforcement Authority ent	Whois (registrant name, contact, location)	Identify location of threat
	Law Enforcement Authority	Whois (registrant name, contact, location)	Identify location of terrorist group supporter in Western European country
	Law Enforcement Authority	Whois (registrant name, contact); DNS records; traceroute	Identify server location used by a foreign terrorist group
	Law Enforcement Authority	Whois (registrant name, contact, location)	Identify location of terrorist group supporter and communication conduit in Western Europe
	Law Enforcement Authority	Whois	Internet based threat against US troops based in a foreign country.

	Law Enforcement Authority	All information	WHOIS information has been essential in being able to connect what otherwise would have appeared to be multiple separate fraudulent schemes to a single actor. It is a crucial tool particularly in wide sweeping identity frauds and lack of the WHOIS resource will undermine our ability to investigate and prosecute identity fraud and protect our citizens from such schemes.