Homeland Security Investigations - Office of Intelligence
Rules of Behavior for Accessing Commercial Digital Location Data Services

The ICE Homeland Security Investigations (HSI) Office of Intelligence (Intel) is permitted to use (b) (7)(E) with consent by the user, to support investigative and law enforcement intelligence activities, (b) (7)(E) (b) (7)(E) .

These rules of behavior (rules) apply only to HSI Intel personnel and personnel detailed to HSI in an intelligence capacity. Users must complete and sign the rules of behavior before accessing (b) (7)(E)

These rules apply to all system resources (e.g., laptop computers, smartphones, and portable electronic devices/PEDs) and to the access, receipt, transmittal, and storage of sensitive information related to the applications. The rules also apply to all printing, scanning, and emailing products directly related to use of the applications.

These rules apply to intelligence personnel at the designated workplace and at any alternative workplaces and while on official travel or temporary duty. These rules are consistent with DHS and ICE policies, all applicable Federal laws and regulations, and local policies. Written guidance cannot cover every contingency; therefore, consultation with intelligence management, use of best judgment, and highest ethical standards must be applied while using unattributed resources.

For the purpose of this document, “authorized personnel” are ICE personnel, such as intelligence personnel (Chief Intelligence Officers (CIO), Criminal Analyst (CA), Supervisory Intelligence Research Specialists (SIRS), and Intelligence Research Specialists (IRS), Intelligence Operations Specialist (IOS) with the 0132 job series designation). Personnel assigned as Task Force Officers (TFO) or Task Force Personnel (TFP), U.S. Military personnel, student interns and DHS Science and Technology analysts that are designated as authorized users must research activities under the guidance of authorized ICE intelligence management or designated personnel, such as Group Supervisors or Special Agents with the 1811 designation.

Law Enforcement Geospatial Research Activities

(b) (7)(E)

Homeland Security Investigations - Office of Intelligence
Rules of Behavior for Accessing Commercial Digital Location Data Services

(b) (7)(E) [redacted]

1. Use of Commercial Location Data Services and Applications

Hardware and Software Applications

- I understand that I am given access to only those systems for which I require access to perform my official duties and for purposes that are authorized by statutes, executive order, regulation, or policy.
- I will not attempt to use systems or applications that I am not authorized to access, or violate DHS and ICE policy or guidance.
- I will only access those sites for which I require access to perform mission-related tasks as part of my official duties and for purposes that are authorized by statutes, executive order, regulation, or policy.
- I will only use approved equipment (government issued/obtained in the course of official duties, stand-alone, etc.), and approved internet connections (b) (7)(E) [redacted]
- I will not attempt to manipulate the hardware or software applications in any way other than the manner in which the applications are provided by authorized personnel.

Privacy and Compliance Protection

- I will not access information that is not publicly available without consent, unless authorized by warrant in the execution of the terms of my assigned mission responsibilities.
- I will protect any personally identifiable information (PII) derived from/or enhanced by, the commercial data research in accordance with the Privacy Act (where applicable) and DHS and ICE privacy policy.
- I will only collect and use the minimum amount of PII necessary for the defined mission-related and official use capacity.
- I will protect sensitive information from disclosure to unauthorized persons or groups.
- I will not access, process, or store classified information on equipment that has not been authorized for such processing.

Homeland Security Investigations - Office of Intelligence
Rules of Behavior for Accessing Commercial Digital Location Data Services

- I will log off or lock my workstation or laptop computer, or I will use a password protected screensaver, whenever I step away from my work area, even for a short time; I will log off when I leave for the day.

Teleworking (Working at Home or at an Alternation Work Location)

Employees approved for teleworking must adhere to the following rules of behavior:

- At my alternate workplace, I will follow security practices that are the same as, or equivalent to those required of me at my primary workplace.
- I will physically protect any laptops or PEDs I use for telecommuting when they are not in use.
- I will protect sensitive data at my alternate workplace. This includes properly disposing of sensitive information (e.g. by shredding).

2. Intelligence Internet Activities

- Intelligence personnel will consult with criminal investigators (case agents) regarding the planned methods and techniques(b) (7)(E) [redacted]

3. General

Accountability

- Users understand that they have no expectation of privacy while using the system.
- Users understand that they are made accountable for their actions through automatic system audit logs that record all actions taken while accessing and using the system.

Miscellaneous Rules

- Users are not permitted to replicate or store information gathered in a separate database or in any other electronic format other than DHS-approved equipment.
- Users will ensure that their workstations have DHS-approved anti-virus software enabled and operating at all times.

Non-Compliance

- Failure to follow these rules will result in consequences for non-compliance, such as verbal or written warnings, removal of system access, reassignment to other duties, disciplinary action, and/or criminal or civil prosecution.

Homeland Security Investigations - Office of Intelligence
Rules of Behavior for Accessing Commercial Digital Location Data Services

- Any non-compliance incident may be escalated to a security violation.

Incident Reporting

- I will promptly report suspected or confirmed IT security incidents (e.g. compromise of user names and passwords or infection with malware, Trojans, or key logging software), as per the DHS Handbook for Safeguarding Sensitive PII and the Privacy Incident Handling Guide (PIHG), and report privacy incidents (e.g. loss or compromise of PII) to the ICE Service Desk at (b) (7)(E) and my immediate supervisor.
- I will immediately report any incidents to the applicable group supervisor and responsible HSI Intel management.(b) (7)(E)

Acknowledgment Statement

I acknowledge that I have read the rules of behavior, I understand them, and I will comply with them. I understand that failure to comply with these rules could result in a verbal or written warning, removal of system access, reassignment to other duties, criminal or civil prosecution, or termination.

Name of User		I&A Branch	
User ID		Location (physical address	
User Phone Number		Supervisor Name	
User email address		Supervisor Contact Information	

---------- ----------
Signature Date