DRAFT

Vehicle & Mobility Security Data Logging Standard

1 Summary

1.1 Purpose

- Identify events and actions in the vehicle and related cloud-hosted and mobile application environments that must be logged.
- Establish high-level requirements to support activity logging as an effective and auditable security control.
- Define system activities and events that must be included when configuring and collecting connected vehicle and mobile application log data.
- Set appropriate baseline retention schedule for logged data.

1.1.1 Rationale

Log collection and subsequent log examination is a detective control that enables discovery of abnormal or anomalous activities after they have occurred. Goals include early incident detection and response, and preventing or mitigating against similar activities in the future.

The subsequent review of collected log data provides a mechanism to ensure proper change management during events such as Over the Air (OTA) updates, changes to system configurations, application libraries and user privileges, and so on.

Other uses for security logging include ongoing validation of controls effectiveness, forensic analysis, alert generation, accountability for actions, vulnerability management, fleet telematics and customer-facing initiatives.

1.2 Scope

This standard applies to all Company-managed or Company-developed services and features in the Business-to-Consumer (B2C) mobile application and Connected Vehicle environments.

Collected and logged data must comply with regulatory and legal requirements in each Global market for vehicle data collection, privacy, user tracking, and driving behavior.

1.3 Out of Scope

Log formats, logging APIs, specific repositories and tools, and log transmission methods are beyond the scope of this Standard.

1.4 Roles and Responsibilities

1.4.1 Vehicle & Mobility Security (Ford Cyber Security)

- Identify and relay minimum vehicle and mobility data collection and logging requirements, including those mandated by law, to other stakeholders.
- Understand and approve decisions made regarding security log generation and review. Such considerations include but are not limited to cost, ability to track or not track accountability, early detection of incidents, and incident response plans.

1.4.2 Product Development and Application Development Teams

- Work with Vehicle & Mobility Security and other stakeholders to determine log management requirements.
- Implement log management requirements as approved, in accordance with the Ford Information Security Policy (ISP) and associated standards-based requirements.
- Provide implementation details and cost implications to Vehicle & Mobility Security.

1.4.3 Cyber Security Center (Ford Cyber Security)

- Ensure tools used to collect and process logged data align with this standard.
- Inform other stakeholders of gaps in the data received for incident management and data forensics, and any collected data elements deemed redundant and/or unnecessary.

2 Standard

Many data elements can be collected in multiple ways. For example, the Basic Safety Message (BSM) integral to Vehicle-to-Vehicle (V2V) includes data elements also needed for security logging; once implemented, logging BSM data may supersede a requirement to log that same data from other sources.

2.1 Event Logging Summary

Log collection enables visibility into connected vehicle and mobility operations, to validate controls effectiveness, conduct forensic analysis, generate alerts and support accountability for actions.

Where feasible, transactional logs must be captured using centralized tools, such as event registries. Subsequent monitoring and analysis should be able to identify abnormal patterns and aid in detection of fraudulent activity.

2.2 Common Logging Requirements

The following subsections identify areas or situations where logging must be implemented.

2.2.1 Common Fields

- **Date/Time**: All logs must include the date, time, and offset from UTC that the event occurred.
- **User ID:** The user ID (vehicle owner, mobile app user, etc.) associated with the event. Where users must opt-in to share this data, resulting logs may omit this field.
- **Session ID:** Unique identifier (token or key) for the session when an event occurs.
- Other common fields to consider: Event/Error message, User IP, Service/Resource name, Service/Resource accessed IP, Service/Resource URL.
    - *Examples:* Application ID (AppID); Developer ID (DevID); ConnectFlag

2.2.2 Cloud Service Elements

Where a mobile application or vehicle system stores or retrieves data from a cloud service (Ford-managed or third party), these data elements must be logged:

- Subscription status (Broker authentication, FordPass subscription, etc.)
- Operating System (OS) status
- Authentication attempts
- Successful authentication of user credentials (user proves their identity)
- Unsuccessful authentication (such as incorrect PIN entries leading to purging of stored username and password credentials and/or authentication tokens)

2.2.3 Mobile Application Elements

A mobile app security event log shall include:

- Mobile OS state and status
- Installed application inventory (where allowed by Device Owner)
- Carrier firmware state and status
- Sensitive data access
- Authentication attempts (successful and unsuccessful, if distinct from cloud service)
- Credential lockout
- PIN lockout events (Device PIN, App PIN, FP/FCIS, BLE, etc.)

2.2.4 Authorization

Logging authorization and access attempts must be based on the value and function of the vehicle system, application and/or data involved, and shall include:

- Vendor authorized commands
- Cloud authorized cellular commands
- Successful access attempts (user allowed to perform specified actions)
- Unsuccessful access attempts (user denied ability to perform attempted activity)

2.3 System Policy/Configuration Changes

System configuration changes must be logged, including Over-the-Air (OTA) updates, requests and failures.

2.3.1 Exception Flags

Where a configuration parameter range is set up, development teams should raise flags for exceptions. *Examples:* Flag when internal, vendor and/or supplier configuration files are accessed, changed or modified without authorization or outside the change process.

2.3.2 Monitoring User Lists

When monitoring users, log the unauthorized addition or deletion of users, especially those with administrative and/or elevated privileges.

2.4 Vehicle-Related Logging Requirements

2.4.1 Vehicle Owner (Administrator) Activity

Activity related to ownership or authorized usage of a connected vehicle must be logged, including the following events:

- Pairing a new mobile device to a vehicle
- Adding a new vehicle to an existing mobile application account
- Creation of new users (authorized drivers, etc.)
- Removal of existing users
- Granting increased or reduced rights to an authorized user
- Delegated authentication/authorization
- Creation of user groups (where applicable, such as fleet telematics)
- Addition/removal of users to groups
- Deletion of users or groups
- Password changes initiated by vehicle owner (administrator) for the mobile app or the vehicle

Note: *Additional administrative activity logging may also be necessary if required as part of the systems documented controls, or as deemed necessary by Ford Cyber Security.*

2.4.2 Vehicle Component System Elements

- Body Control Module (BCM) serial number and lifecycle mode
- Enhanced Central Gateway (ECG) serial number and lifecycle mode
- Ethernet device/frame MAC Address
- SYNC ID
- Vehicle location where such information complies with PII, SPII and/or GDPR rules
- Vehicle state
- Infrastructure / environment changes
- Vehicle System data – startup, shutdown and overrides
- Where an active tap is installed, collect generated logs in accordance with this Standard.

Note: *For Ethernet devices, the MAC Address may serve as the unique device identifier.*

2.4.3 Vehicle Telematics Data

Data collected by the vehicle during operation is critical to determining abnormal, anomalous or malicious behavior. All vehicle telematics data may be logged; at a minimum, vehicle telematics security logs must include these data elements and triggers:

Data Elements	Key ON	Every 2 min	On Event Trigger	Collected per Country
Date	X	X	X	All
Time	X	X	Most Events	All
Vehicle Identification Number (VIN)	X	X	X	All
Vehicle alarm status & trigger	X		Some events	All
GPS (location) where appropriate	X	X	Most Events	USA, CAN, EU-20
Paired mobile device usage	X	X	Most Events	All
Driver Alert System (DAS) activity	X	X	Most Events	All
Driver Alert System disabled	X	X	Most Events	All
Motive mode (engine status)	X		Some events	All
Remote start status and duration	X		X	All
Key in use (Passive Entry/Passive Start)	X			All
Advanced Driver Assistance Systems (ADAS) for AV	TBD	TBD	TBD	TBD
V2X Basic Safety Message (BSM)	TBD	TBD	TBD	TBD

2.5 Log Management

When using event log generation and subsequent data review as a point of control, such use must be listed in the appropriate control review document (e.g. Statement of Accountability (SoA) at https://it2.spt.ford.com/sites/ITSecurity/process/Pages/ACR.aspx).

Log management procedures must be established in accordance with the following sections before vehicle, related cloud service and/or mobile app event logging (with log reviews) can be considered an effective control.

2.5.1 Access Control

- Access to logs must be limited based on a need to know as documented in the appropriate specification or control review.
- Separation of duties must be established to prevent unauthorized changes to logs.
- Where feasible, access control logs must be used to determine which access control mechanism was compromised to gain unauthorized access:
    - Monitor both authorized and unauthorized access.
    - Monitor for excessive escalated/privileged accounts.

2.5.2 Retention Requirements

Log data with significant value as a detective security control, and all common logging requirements (see **2.2** above), must be securely retained for thirty (30) days unless otherwise documented.

- Data should not be stored on endpoints (vehicles, mobile devices). Connected vehicles should have 100% connectivity at all times; there should be no need to store log data for batch uploads to the backend systems.
- Additional retention requirements must be documented in the appropriate specification or control review.

Unless otherwise indicated, retained log data are Transient records under the Ford Global Information Management (GIM) protocol (https://ogc.spt.ford.com/sites/GIM/Pages/Default.aspx).

2.5.3 Log Review Procedures

Log review procedures must be established and must include (but not be limited to) identification of abnormal or anomalous security events.

- Log review frequency must be predefined, and performed often enough to ensure logs are neither purged nor overwritten between review periods.
- Log review occurrences must be documented.

Abnormal or anomalous security events must be reported to the Cyber Security Center (CSC) for review and possible investigation.

2.5.4 Escalation of Log Review Findings

Escalation procedures must be established to resolve abnormal or anomalous security events identified during log reviews.

3 Appendices

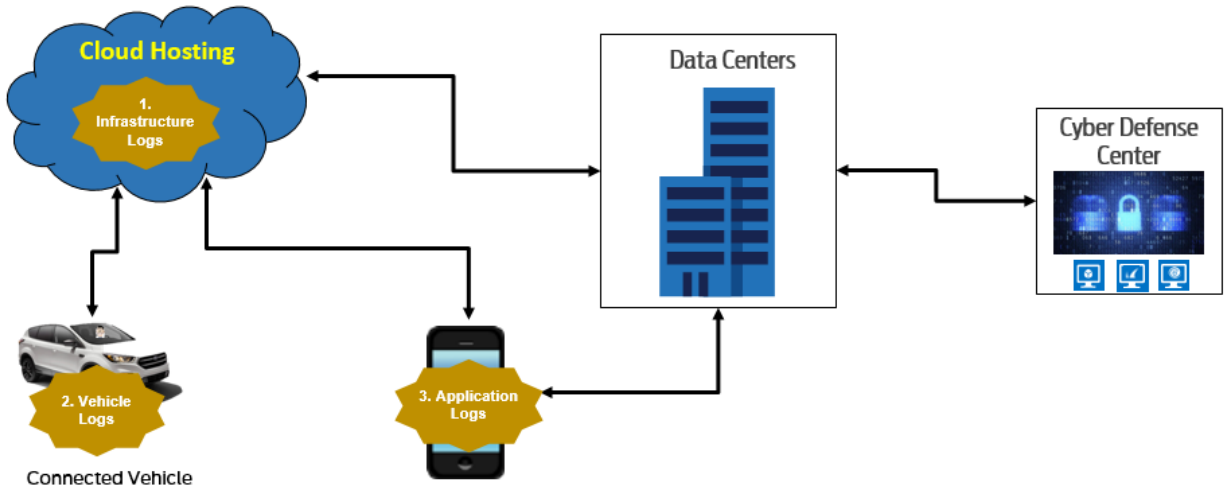
3.1 References

- Information Security Policy – pages 63-65
- Information Systems Security Logging Standard

3.2 Log Examples

Type of logs	Examples
System logs	• System activity logs (e.g. Administrator), including storage • Operating System Updates logs • Endpoint (and agent-based) logs (e.g. Symantec Antivirus, Microsoft System Center) • Logs from standard (e.g. SAP) and customized applications • Authentication (e.g. Windows, System, Application) logs • Physical security logs
Networking logs	• Email, firewall, VPN and Netflow logs
Technical logs	• HTTP proxy logs • DNS, DHCP and FTP logs • Web and SQL server logs • Appflow logs • Wireless data logs from CAN-connected devices (Ethernet, Bluetooth, etc.)
Logs from cyber security monitoring and logging tools	• Malware protection (e.g. anti-virus) logs • Network intrusion detection systems (NIDS) • Network intrusion prevention systems (NIPS) • Data loss protection (DLP) • Tools that employ potential malware isolation and investigation techniques (e.g. sandboxing or virtual execution engines) • Other relevant security management appliances or tools

3.3 Sample Logging Work Stream



4 Revision History

Change Date	Change Description
28 Feb 17	Initial Drafts
4 May 17	Reviewed content, minor changes
13 Dec 17	Updates for sharing with internal teams; added references to SCA-V and related systems
16 Jan 18	Reviewed, minor changes throughout; added Appendices, Log Examples, Logging work stream diagram
1 Mar 18	Updated based on feedback received.
4 Apr 18	Suggested changed and clarifications throughout.