Vetting Mobile Applications for Federal Agencies: NIST AppVet and DHS Carwash

Steve Quirolgico
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Doug Hansen, Chris Drew, Anthony Glynn
Enterprise Systems Development Office
Office of the Chief Information Officer
Department of Homeland Security

FCSM
January 28, 2016

Agenda

- **NIST AppVet**
  - History
  - App Vetting
  - System Overview
  - Impact on USG Operations

- **DHS Carwash**
  - Overview
  - Transition of AppVet to Carwash
  - Using Carwash

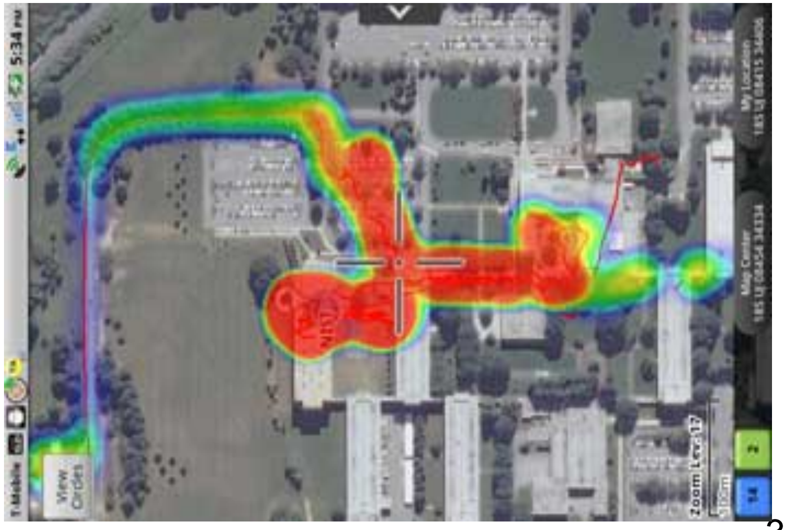
DARPA Transformative Applications (TransApps)

DARPA TransApps focused on the use of smartphone applications (apps) for tactical use.

TransApps applications:

- Provided mission-critical, leading-edge capabilities:
  - Weaponry/Munitions
  - Medical/First-Aid
  - Cultural/Language
  - Mapping/Recon/Logistics
  - Tactical Information Sharing
- Significantly improved combat operations
- Saved the lives of U.S. soldiers

Army

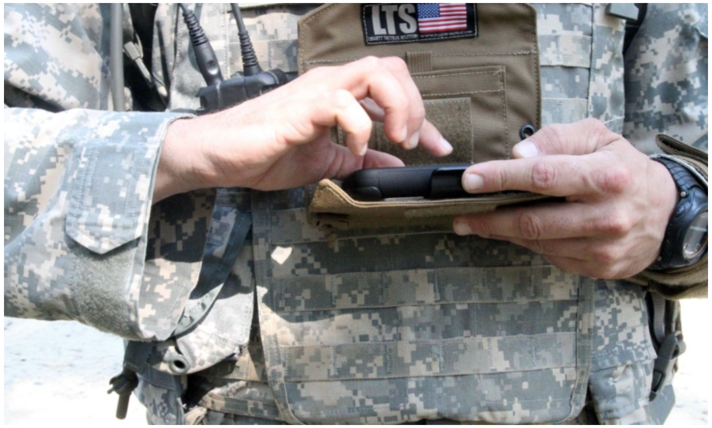


TransApps Security

Security of smartphone technologies was crucial for protecting sensitive information and ensuring proper operation.

Security needed to prevent:

- Unauthorized access to PII, geolocation, or other sensitive data
- Unauthorized network communication
- Unauthorized audio/video recording
- Unintended app or device behavior
- Resource (memory, CPU, *etc.*) exhaustion
- Shortened battery life
- **Mission failure**



Achieving TransApps Security

Two Efforts:

- Hardware/OS
- Software Applications (Apps)

Hardware/OS Security

Focused on the development of hardened COTS Android devices (referred to as PANTHR devices).

- **Modified Android OS**
- **Hardware Security Stack**
  - CVE Patched Linux Kernel
  - Data At Rest Protections
  - Data In Transit Protections
  - Device Integrity Checks
  - Device Authentication

Software Application (App) Security

Focused on securing software applications for tactical use.

Three Efforts:

- **Functional Testing:** Assess that apps performed only their intended functionality
- **App Vetting (NIST):** Assess the security* of apps
- **Acquisition**: Develop an app store for downloading only vetted apps onto secure PANTHR devices.

*Determining the security of an app may help to determine the app's reliability, efficiency, etc.

What is App Vetting?

App vetting is a process for assessing the security of an app for deployment on an organization's devices

Two main focuses:

1. Assess the security of an app through vulnerability testing
2. Assess the compliance of an app with organizational security policies (usually regarding usage)

App Vulnerabilities Overview

- Vulnerabilities, if exploited, can result in serious security-, reliability-, and efficiency-related issues.
- Thousands of vulnerabilities exist for both Android and iOS apps.
- On average, an app contains approximately 14 vulnerabilities.*
- Vulnerability types include those related to:
  - Incorrect Permissions
  - Exposed Communication
  - Dangerous Functionality
  - Traditional Software Vulnerabilities

*Cenzic, *Application Security Trends Report*, 2014.

App Compliance with Security Policies

- App compliance determined by examining organizational vetting criteria against organizational security policies
- Organizational vetting criteria includes:
  - Information about an app's capabilities/functionality
  - Information about the organization's target users, deployment environments, *etc*.
- Example organizational security policies:
  - Social media apps are not permitted on any device
  - Apps that record audio or video are not permitted in secured areas (e.g, SKIF)
  - Classified apps must only be used by classified personnel

App Vetting Process

App vetting comprises 5 activities:

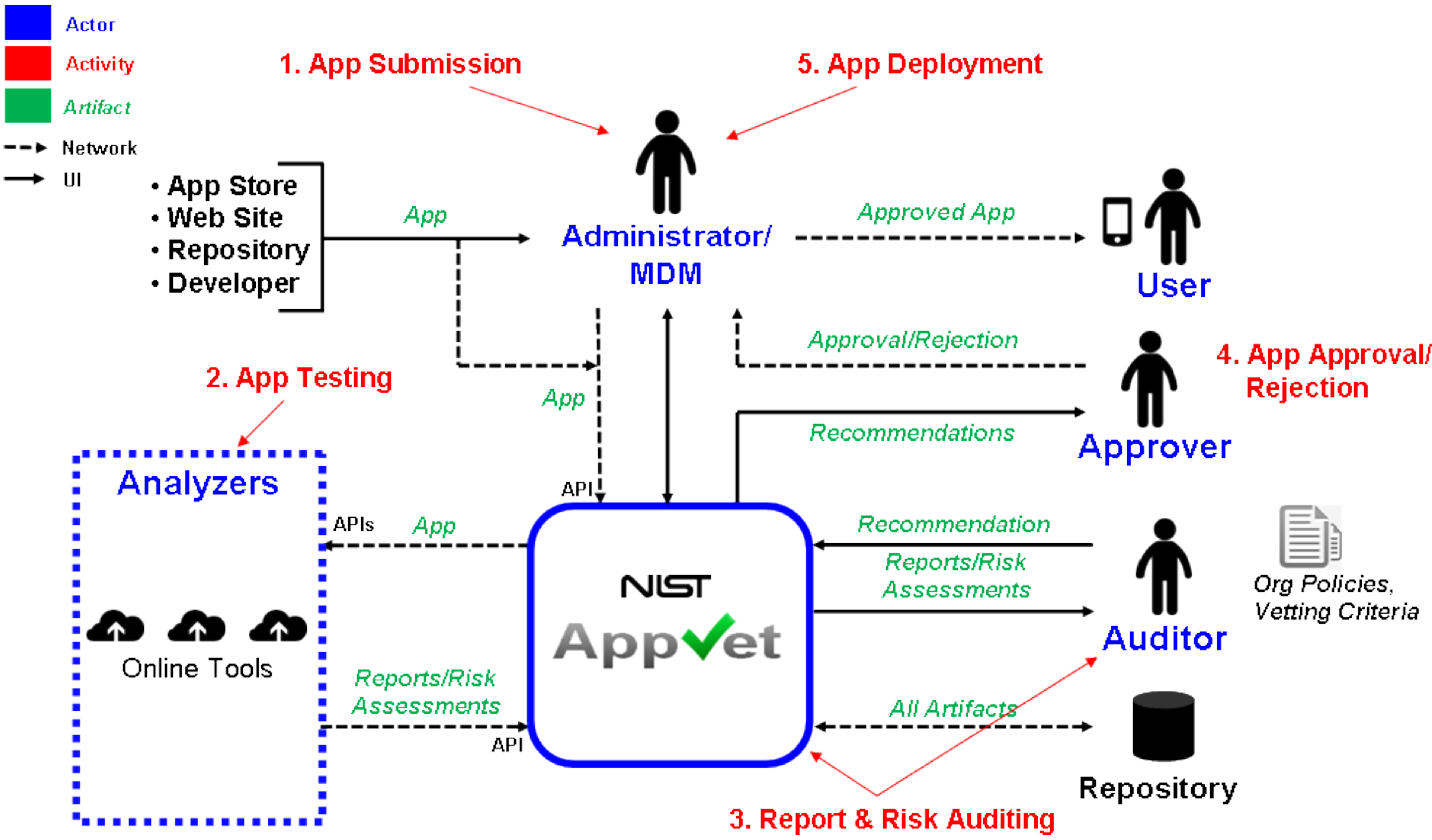
1. **App Submission:** Submission of app from Admin/MDM to an Analyst who manages the app vetting process.
2. **App Testing:** Testing of app by an Analyst through multiple Analyzers (standalone tools, online testing services, etc.).
3. **Report and Risk Auditing:** Inspection by Auditors of reports and risk assessments generated by Analyzers. Auditors also examine app's compliance to organizational requirements to provide a recommendation for app approval/rejection.
4. **App Approval/Rejection:** Examination by Approver of recommendations provided by Auditors. Approver provides official organizational approval/rejection.
5. **App Deployment:** Deployment of app by Admin/MDM based on approval from Approver.

AppVet

AppVet is a system for managing and automating the app vetting process

- Automates most app vetting activities
- Defines APIs and protocols for integrating third-party, distributed online testing services and clients (e.g., app stores)
- Support storage management of artifacts
- Supports enterprise-level management
- Provides a web-based user interface for manually managing app vetting activities

AppVet System Overview



🟦 Actor
🟥 Activity
🟩 Artifact
- - ► Network
→ UI

1. App Submission

5. App Deployment

- App Store
- Web Site
- Repository
- Developer

App

Administrator/ MDM

Approved App

User

Approval/Rejection

4. App Approval/ Rejection

2. App Testing

App

Recommendations

Approver

API

Analyzers

APIs

App

NIST AppVet

Recommendation

Reports/Risk Assessments

Auditor

Org Policies, Vetting Criteria

Online Tools

Reports/Risk Assessments

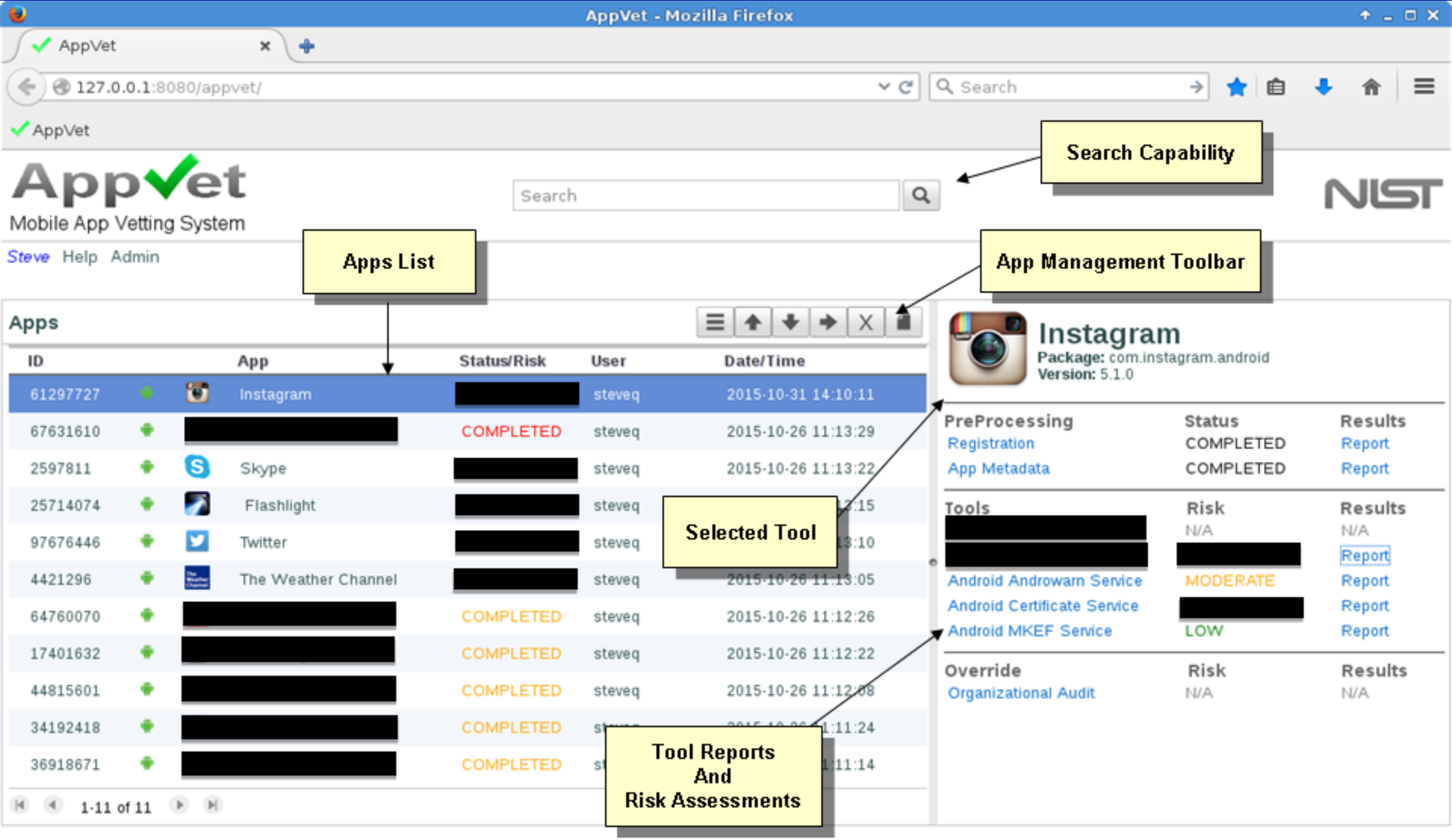
All Artifacts

API

Repository

3. Report & Risk Auditing

AppVet User Interface*



Search Capability

Apps List

App Management Toolbar

Selected Tool

Tool Reports
And
Risk Assessments

Apps

ID	App	Status/Risk	User	Date/Time
61297727	Instagram	[redacted]	steveq	2015-10-31 14:10:11
67631610	[redacted]	COMPLETED	steveq	2015-10-26 11:13:29
2597811	Skype	[redacted]	steveq	2015-10-26 11:13:22
25714074	Flashlight	[redacted]	steveq	:15
97676446	Twitter	[redacted]	steveq	3:10
4421296	The Weather Channel	[redacted]	steveq	2015-10-26 11:13:05
64760070	[redacted]	COMPLETED	steveq	2015-10-26 11:12:26
17401632	[redacted]	COMPLETED	steveq	2015-10-26 11:12:22
44815601	[redacted]	COMPLETED	steveq	2015-10-26 11:12:08
34192418	[redacted]	COMPLETED	st	1:11:24
36918671	[redacted]	COMPLETED	st	1:11:14

1-11 of 11

Instagram
Package: com.instagram.android
Version: 5.1.0

PreProcessing	Status	Results
Registration	COMPLETED	Report
App Metadata	COMPLETED	Report

Tools	Risk	Results
[redacted]	N/A	N/A
[redacted]	[redacted]	Report
Android Androwarn Service	MODERATE	Report
Android Certificate Service	[redacted]	Report
Android MKEF Service	LOW	Report

Override	Risk	Results
Organizational Audit	N/A	N/A

*UI is currently being revised.

AppVet Impact on USG Operations

- Vetted apps deployed on >3000 devices for military and security-related operations:
  - Afghanistan (2011-Present)
  - Presidential Inauguration (2013)
  - Boston Marathon (2013-2014)
  - Other USG operations (2011-Present)
- Helped enable the detection of numerous vulnerability, reliability, and power consumption issues in commercial, open-source, and USG-developed apps
- Helped enable the DOD to deploy modified commercial solutions, reduce development costs, and enhance combat capability for U.S. troops

DHS Carwash Overview

- Provides government development teams with a continuous integration build, testing, source code management, and issue tracking for building applications
- Working to tie into federal Mobile Device Mangers (MDMs) to help provide vetted applications and provide a monitoring service to provide updates to customers about new app versions and vulnerabilities of apps
- Supports a number of COTS, open source, and USG-developed app testing tools
- Sponsored by DHS OCIO
- Fully accredited system with Authority to Operate (ATO)
- Open to all federal agencies

AppVet Transition to DHS Carwash

- AppVet will provide complementary app vetting capabilities to DHS Carwash
- Transition Phases:
  - Development, Integration, and Customization:
    - Integrate into DHS Carwash environment
    - Develop and customize to support DHS requirements
  - Testing:
    - Security
    - 508 Compliance
    - Performance, reliability, efficiency, and functionality
  - Deployment
- Full Transition Date: TBD

Carwash FAQ (1 of 3)

- **Is Carwash open to all federal agencies?** Yes, in a limited-use capacity. Use outside of DHS is approved on a case by case basis.
- **What is the cost of using Carwash?** In its current configuration, there is no cost for DHS users. DHS currently has agreements with a limited number of other USG agencies to provide this service. The only costs that would be passed to customers would be for COTS licenses for specific scanning tools that the agency wants to use.

Carwash FAQ (2 of 3)

- **What platforms will be supported?** Android and iOS. Additional platforms may be supported dependent on need and likely requires funding.
- **Is there a limit on the number of apps that can be submitted for processing?** This is determined on a case by case basis and depends on the agreement with the customer/agency.
- **Will DHS certify an app as "safe"?** No. Carwash provides test results back to the user, and the risk determination is the responsibility of the requester and their organization.

Carwash FAQ (3 of 3)

- **Will users require a special account to access Carwash?** Yes, users will require accounts to access Carwash. New organizations and projects must establish a Letter of Intent (LOI) and populate a new project request. This requires a federal lead/sponsor and security POC for the project.
- **Will results for my app be available to other agencies?** Not unless allowed by app owner/uploader.

Carwash Website and Contact Information

- **Website (Note, you must have an OMB MAX account to access):**

  https://community.max.gov/pages/viewpage.action?spaceKey=DHSExternal&title=DHS+Carwash

- **Contact:**

  Doug Hansen
  DHS/OCIO/MGMT/ESDO
  Doug.Hansen@HQ.DHS.GOV
  Or
  Carwash@hq.dhs.gov