



**Oregon Department of Transportation**

---

## **Enterprise Security Fabric**

### **Project Charter**

Approved by

A handwritten signature in black ink, appearing to read 'Lorna Youngs'.

Lorna Youngs  
Deputy Director  
Central Services Division

**Version: 2.0**

Date: 02/17/08

Status: Approved

## Background

The Oregon Department of Transportation (Department) recognizes that its information assets are valuable and essential to its mission. The Department must provide information assets conveniently for authorized purposes and protect them from unauthorized disclosure, modification, or destruction.

The Oregon Consumer Identity Theft Protection Act (ORS 646A.600) (the Act) -- provides consumers with more tools to protect themselves against identity theft and Oregon businesses, including state government, must comply with standards to ensure the safety of the personal identifying information they maintain. Personal information includes a consumer's name in combination with a Social Security number, drivers' license number, financial account, or credit or debt card number along with security or access code or password that would allow access to a financial account.

The Act requires any business, organization, or individual, including state government, which maintains personal information of Oregon consumers to notify their customers if computer files containing that information have been subject to a security breach. (Although the Act limits notification to computer files, the Department understands that notification will be required on any breach of personal information.) Businesses will also be prohibited from printing Social Security numbers on cards or documents, or publicly display or post them. Businesses or organizations, including state government, that collect personal information must develop, implement and maintain reasonable safeguards to protect the security and confidentiality of the information.

The Department of Administrative Services (DAS) has been designated as the "single point of accountability" for information security at the state (ORS 182.122).

In support of this mandate, the DAS Enterprise Security Office (ESO) is instituting a security strategy wherein DAS works collaboratively with state agencies to ensure the state's security posture is at an acceptable level. Information security management enables information to be shared while ensuring protection of that information and its associated technology assets. To assist in this effort, DAS has implemented a set of essential enterprise information security policies, the purpose of which is outlined below:

- Represent a baseline minimum necessary level of security that agencies must conform to.
- Set the direction and define requirements for information security-related processes and actions across the state enterprise.
- State the minimum requirements to establish and maintain a secure environment, and achieve enterprise security objectives.
- Emphasize the state's commitment to information security.
- Establish clear expectations for staff performance, behavior and accountability.

The following policies establish standards and guidelines related to the identification, management and protection of information assets for state agencies. These policies will be referred to hereafter as "DAS policies".

<u>Information Asset Classification</u>	107-004-050
<u>Controlling Portable and Removable Storage Devices</u>	107-004-051
<u>Information Security</u>	107-004-052
<u>Employee Security</u>	107-004-053
<u>Transporting Information Assets</u>	107-004-100
<u>Acceptable Use of State Information Assets</u>	107-004-110
<u>Information Security Incident Response</u>	107-004-120

## **Security Fabric Vision and Mission**

### ***Vision***

Everyone working for ODOT recognizes that its information assets are valuable and essential to its mission. ODOT provides information assets conveniently for authorized purposes and protects them from unauthorized disclosure, modification, or destruction.

### ***Mission***

ODOT regularly and systematically assesses risks to its information assets and assures compliance with all related regulations. ODOT proactively manages risks to information assets through coordinated efforts of governance, education, and technology.

### **Charter Statement**

The Department charters the Security Fabric Project to develop an integrated business and security strategy that will provide a common holistic approach to information security. The goal of the Security Fabric Project is to minimize risk to the Department by designing a programmatic approach that ensures compliance with the various laws, policies, and standards governing information assets.

### **Purpose**

The purpose of this project is to:

- Raise the awareness of information security risks and compliance issues among Department staff. This will lead to a higher awareness of information security standards and mature the Department's information security culture.
- Identify compliance requirements for the Department with respect to the Act and the DAS Policies.
- Research, collect, and distribute standards to meet compliance requirements.
- Develop audit processes and tools to be used across Department business lines to identify gaps in compliance with the Act and DAS Policies.
- Transfer knowledge, processes and tools to designated Department staff to assist them in performing information security audits for their respective line of business.
- Provide recommendations for the ongoing identification, protection, and management of Department information assets to Department Executive Staff.

## **Membership**

The Security Fabric Project Team is comprised of:

- Ben Berry, CIO, Executive Sponsor and Interim Co-Chair\*
- Lisa Martinez, SSB Business Services Section Manager, Co-Chair
- Tim Avilla, ISB Enterprise IT Program Architect
- Paula Harr, BSS Records Management Analyst
- Karina Stewart, ISB Security Analyst

It is anticipated that the Project Team membership will include representatives from key Department business areas as the need is defined.

## **Roles and Responsibilities of Members**

- Attend and actively participate in all Project Team meetings and other related activities.
- Provide timely and constructive input to the Project Team.
- Timely and accurately complete all assignments.
- Advise Chair in advance of meeting absences.
- Review agenda and meeting information in advance of the meeting.
- Keep the Security Fabric Project Team informed of issues and activities that relate to or impact the purpose of the Security Fabric Project.
- Assist ODOT staff in identifying and understanding issues related to the security of information assets.

## **Duration of Project**

The Security Fabric Project is expected to be completed by June 30, 2009 with the expectation that the Department will adopt a permanent, long-term approach to the identification, protection, and management of its information assets.

## **Contact Information**

For more information

Lisa Martinez  
Manager, Business Services Section  
355 Capitol Street NE, Room 22  
Salem, OR 97301  
503-986-3273  
lisa.m.martinez@odot.state.or.us

## Changes to the Charter

Changes may be made to the Charter based on recommendations of the Security Fabric Project Team and with the approval of the Director. The Security Fabric Project Team shall review and, if warranted, update this Charter at least biennially.

---

\* Ben Berry serves as Co-Chair on an interim basis pending hire of an Information Security Systems Analyst anticipated in the second quarter of 2009. The Security Fabric Charter will be amended upon hire to reflect the permanent Co-Chair.