Technical Panel
of the
Nebraska Information Technology Commission

Excerpt from Technical Panel Minutes for May 8, 2012

STANDARDS AND GUIDELINES - REQUESTS FOR WAIVER

Department of Roads - Request for Waiver from requirements of NITC 8-302*

Mr. Weakly recommended granting a temporary waiver for 18 months until issues regarding the public forest, active directory and the cloud are addressed. The Security Architecture Work Group will be developing a long term vision for identity management which would be accomplished in phases and endorse it by the NITC.

Mr. Winkle moved to grant the waiver for a period of 18 months. The State Information Security Officer is requested to provide an update to the Panel prior to expiration of this waiver. Mr. Langer Seconded. Roll call vote: Scofield-Yes, Langer-Yes, Weir-Yes, and Winkle-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.

DATE: May 3, 2012

TO: Nebraska Information Technology Commission
ocio.nitc@nebraska.gov

FROM: Nebraska Department of Roads, Business Technology Support Division

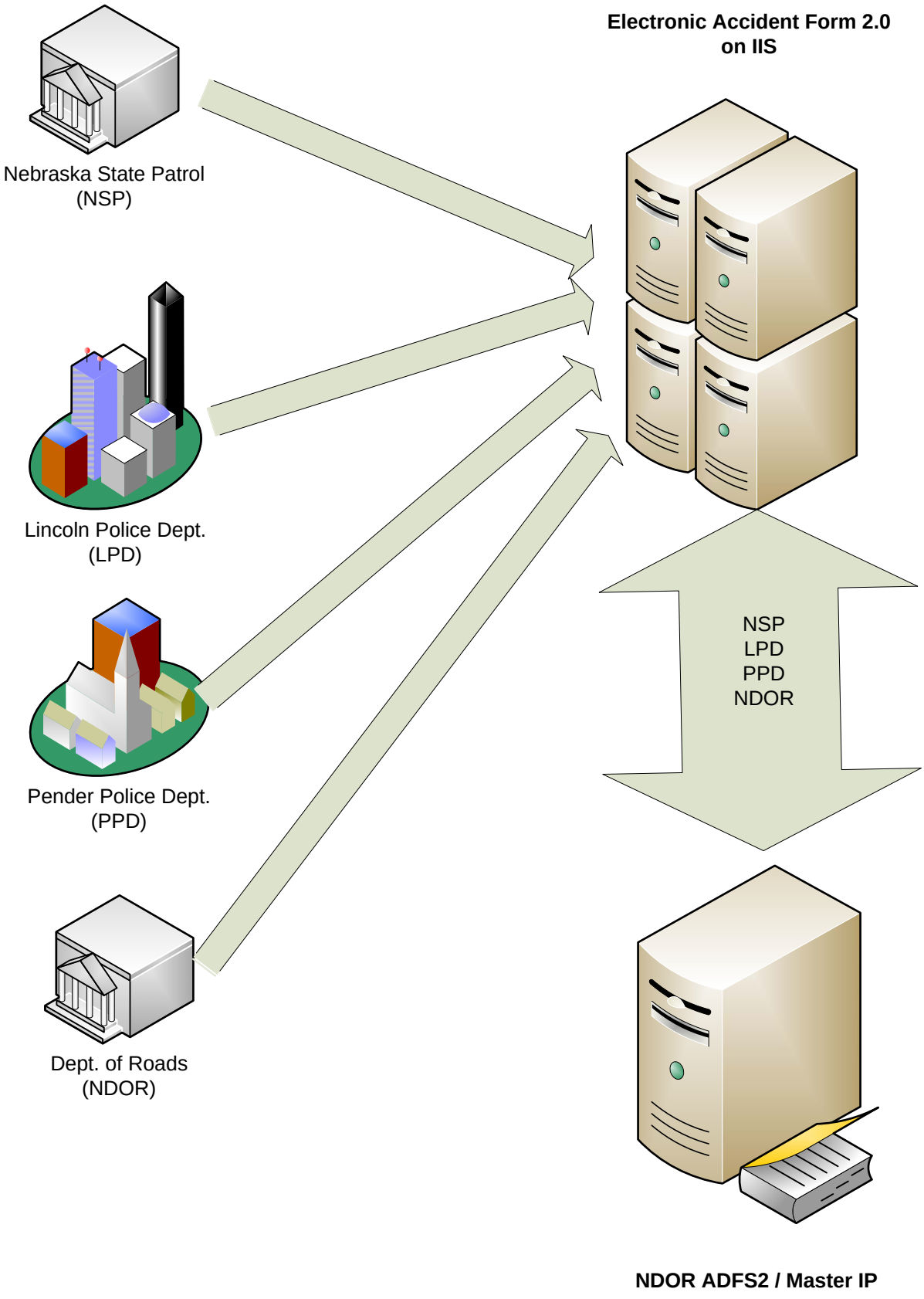
RE: Request for Exemption / Waiver

The Nebraska Department of Roads, Business Technology Support Division (BTSD) requests the committee grant a waiver of Standards and Guidelines, as outlined below:

Requesting Agency and Division	Nebraska Department of Roads, Business Technology Support Division
Name, Title and Contact Information for Requesting Agency	Bill Wehling, NDOR-Engineer VII; bill.wehling@nebraska.gov; 402.479.3986
NITC Standards and Guidelines Document	Identity and Access Management Standards for State Government Agencies (*adopted March 25, 2005*)
Description of the Issue	BTSD is developing a rewrite of the current web based electronic accident form, with a planned deployment of July 1, 2012. The enhanced web application, EAF 2.0, is subject to the standards in section 4.1.1 of the aforementioned document. BTSD is requesting an exemption, as defined in section 4.2, for the following reasons: 1. BTSD is unable to comply with the standards, defined above, for the following reasons: a. The timeline for enhanced OCIO support of ADFS2 infrastructure is not yet defined b. Current application of ADFS2 is limited to one application (Office 365) c. Ramp up, to meet standards, on the part of both teams would require a material investment in resources and a significant delay in the release of EAF 2.0 2. As a stop gap, the EAF 2.0 application has proactively adopted an authentication and authorization process to align with *Identity and Access Management Standards for State Government Agencies* and *Information Security Policy, Section 7 (adopted September 18, 2007)* to include, but not limited to: a. Creation of a standardized, security identification and access management architecture that is centrally managed and locally administered. b. Provides application level authentication and authorization based on the unique identity of the user c. Supports the authentication and authorization of external parties through State standardized Active Directory management processes d. Leverages the latest standards for security in a ASP.NET environment, to include Window Identify Foundation (WIF) requirements 3. The request for waiver/exemption is temporary (see *Additional Supporting Information*, below)
Description of Preferred Solution	
Specific Requirements	The EAF application is a web application that is being re-written in ASP.NET and C# from Java and Servlets. For the EAF our preferred solution for user authorization is the use of Microsoft's WIF. This framework is used along with a group of SQL Server database tables to store complex authorization requirements. WIF is a .NET framework for enabling authentication and authorization based on the concept of claims based identity. It is our goal to utilize all components of the .NET framework since we feel the direction of the State is to be Microsoft-based. Our preferred choice for authentication is ADFS2, a software package from Microsoft that provides authentication services and basic user information for the EAF application. The attached document depicts various types of users for EAF and the separation of the EAF application from the ADFS2 software on a different server. This design satisfies a number of business and design requirements for the EAF application. Including the following: • In order to save time we want to avoid writing additional management pieces for authentication. Specifically:

	○ This choice of software allows us to use our current active directory database to store users. ○ This choice of software allows us to use our current tools to manage users stored in active directory. • We have separated the responsibility for user authentication away from the application. This provides us a number of benefits: ○ We have a flexible framework and pattern that can be repeated by future applications so that they can avoid writing authentication code. Depending on needs , there's an option to also avoid writing custom authorization code. ○ This design would allow us to switch out authentication for multiple applications without re-writing each application as future need arises. ○ This design would allow us to provide authentication from multiple sources as future need arises. This could be done without creating network level trusts. • The use of WIF, ADFS, and claims based technology are important parts of Microsoft's future. ○ Microsoft is integrating the use of ADFS for authentication into current and future software products. Including .NET, SharePoint, and Office 365. • We have user requirements to allow NDOR staff to logon with their current active directory based IDs and to provide IDs for the officers who will use EAF. This solution satisfies both requirements. The design choices made by the EAF today will allow us to use such possible services with little or no change to the EAF application and establish a collaborative foundation with the OCIO to create authentication services specific to the .NET platform and Microsoft on future development.
Additional Supporting Information	1. EAF 2.0 provides a collaborative opportunity, for both BTSD and OCIO, to coordinate and share knowledge of ADFS2 applications and more quickly assess, define and deploy a sustainable and repeatable standard for web based applications, as defined in section 8 of the *Information Security Policy.* 2. The standards developed, either collaboratively using EAF 2.0 as a beta, or independently deployed by the OCIO, would be adopted when feasible and/or available by the EAF 2.0 project.

Reference: Identity and Access Management Standards for State Government Agencies, Section 4.2 (*adopted March 25, 2005*); Information Security Policy, Sections 7 and 8 (*adopted September 18. 2007*); NITC 1-103 Waiver Policy (General Provisions, General Applicability)


Electronic Accident Form 2.0
on IIS
Nebraska State Patrol
(NSP)
Lincoln Police Dept.
(LPD)
Pender Police Dept.
(PPD)
Dept. of Roads
(NDOR)
NSP
LPD
PPD
NDOR
NDOR ADFS2 / Master IP