

# How NIC supports compliance with IRS Pub. 1075

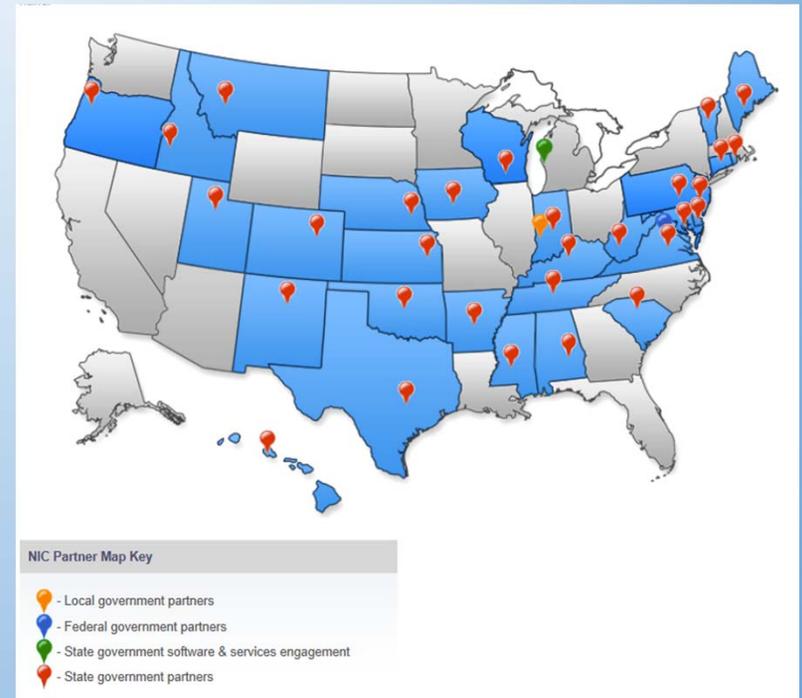


Jeff Walker – General Manager Access Idaho

# Who Is NIC and Access Idaho

NIC - Founded in Kansas and for the past 22 years, NIC has defined the eGovernment industry by building online services for more than 3,500 federal, state, and local government agencies.

NIC has grown steadily each year developing eServices and manages the official Web sites for 27 states and employs more than 725 people across the country. We are a unique company of creative eGovernment specialists and proud to help protect the public trust on behalf of government leaders across the United States.





- Created in 1999 by the State of Idaho to benefit businesses and private citizens.
- Access Idaho (Idaho Information Consortium LLC) is a subsidiary of NIC and is managed at no cost to taxpayers using a self funding model.

2013 in Review

188 Million – Collected Online by Access Idaho

9,517,589 – Transactions completed online 2013

300 – Number of deployed services

The top online revenue activities 2013

Tax	\$69,299,696.97
Labor	\$46,488,079.16
City and County	\$27,131,272.02
Health & Welfare	\$13,250,640.90
Transportation Dept.	\$12,877,837.21
Vehicle Registrations	\$12,032,144.81

113 - Number of county departments we support

41 - Number of agencies we support

32 - Number of city departments we support

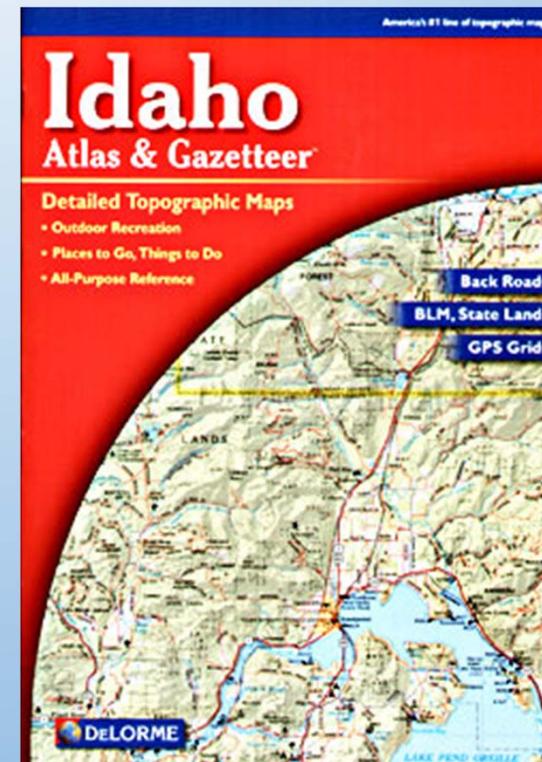
# Security Stance for Access Idaho

- Access Idaho/NIC Corporate Security Policies
  - History
  - Operational areas
- Security Training
  - Who
  - How often
  - Code of Conduct



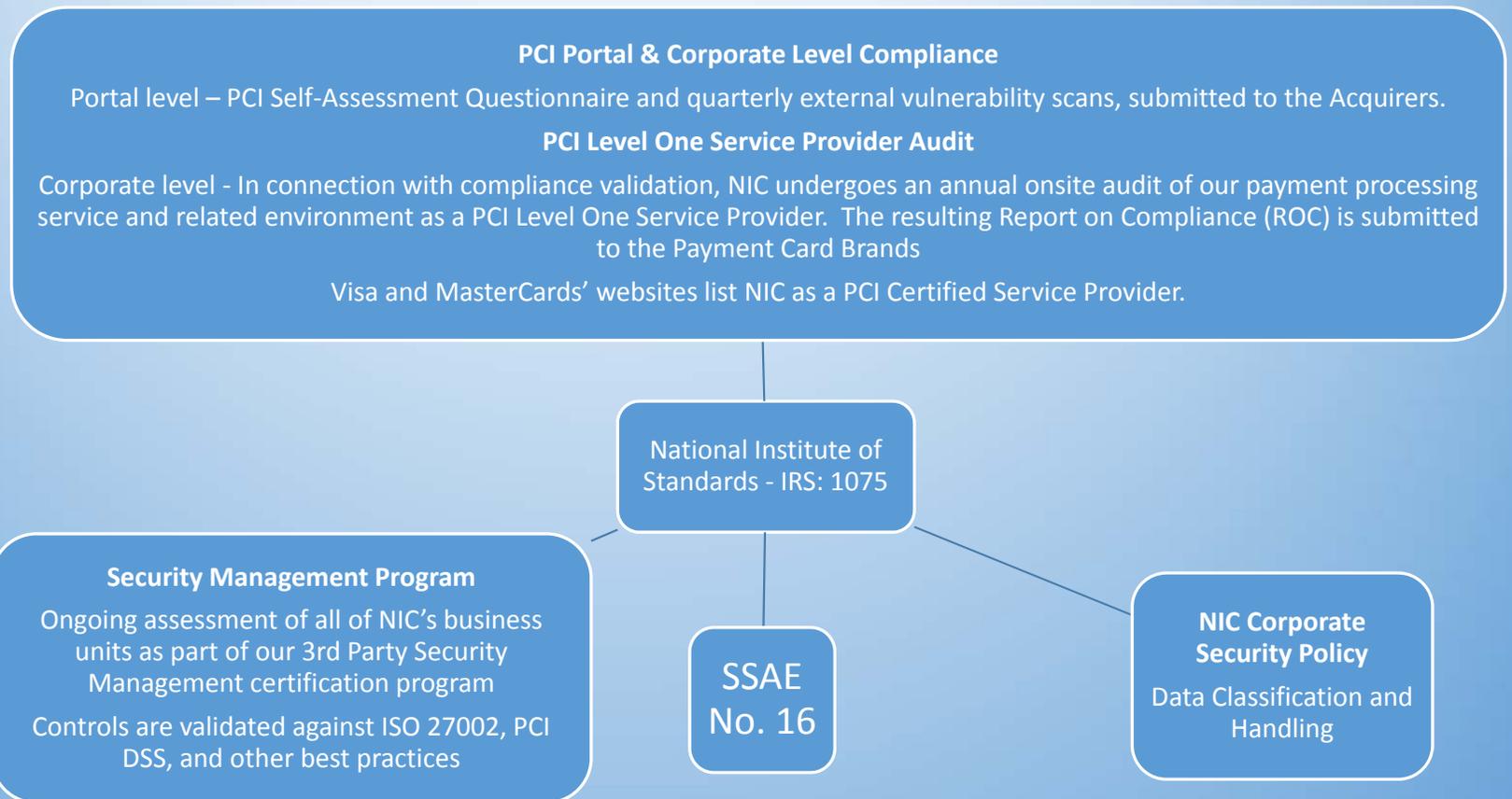
# Mapping of Security Policies to IRS Pub. 1075

- NIC Employee Expectations
  - Partner Confidence
  - Advocates
- Mapping Existing Security Controls to IRS Pub. 1075
  - Gap analysis
  - Policy inventory
  - Existing activity



# Mapping of Security Policies to IRS Pub. 1075

Four core compliance components for mapping to IRS Pub. 1075:



# Data Handling

- NIC Data categories
- Classification & handling review
- Storage and retention
- Sensitive data fields - encryption & truncation
- Encryption & removable media



# NIC's Ongoing Security Practices

Snap shot of what is routinely happening at NIC and its subsidiaries:

- Employee Training on Security Awareness
- Application scanning and remediation
- Penetration testing and remediation
- Quarterly scanning of networks
- Onsite assessments of:
  - Access Control Policy and Procedures
  - Account Management
  - Access Enforcement
  - Separation of Duties
  - Wireless Access restrictions
  - Access Control for Mobile Devices
  - Contingency Planning and documenting Policy and Procedures
  - Physical Access Control
  - Security Alerts, Advisories, and Directives (Disseminated by NIC Security Team to Portal operations)
  - Business Continuity and Disaster Recovery (Annual Test)