



SERC Perspective on CIP Compliance

EEI Security Committee Conference

October 1, 2009



Overview

- CIP Program Perspective
- July 2009 Supplemental Survey
- SERC CIP Spot Check Process
- Enforcement Process Overview
- CIP-004-1: Possible Violation Statistics and Lessons Learned To Date
- Regional Consistency Efforts



CIP Program Perspective

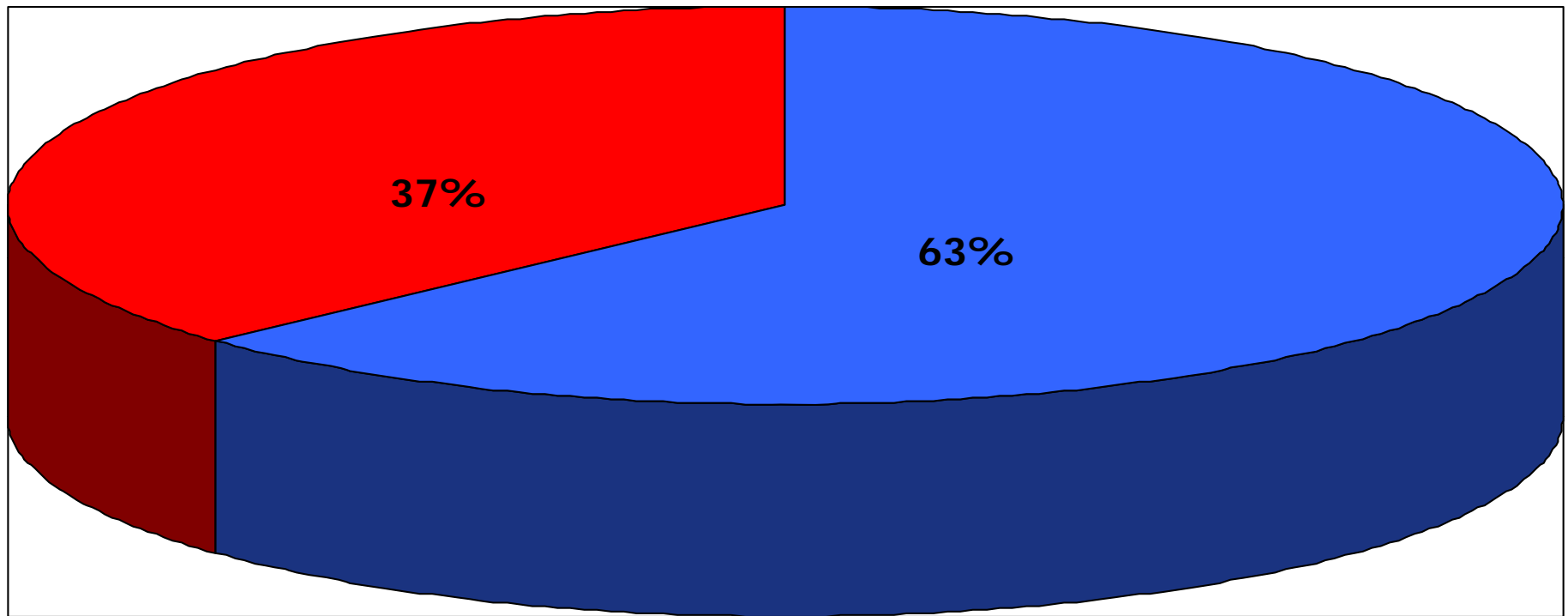
- High Focus (Congress, FERC, NERC, Regions)
- Broad Applicability Across Function Types
- Expansive - 41 Requirements
- Perceived High Risk
 - Demos; Studies; Press
 - Non-traditional Risk
 - Potential Consequences



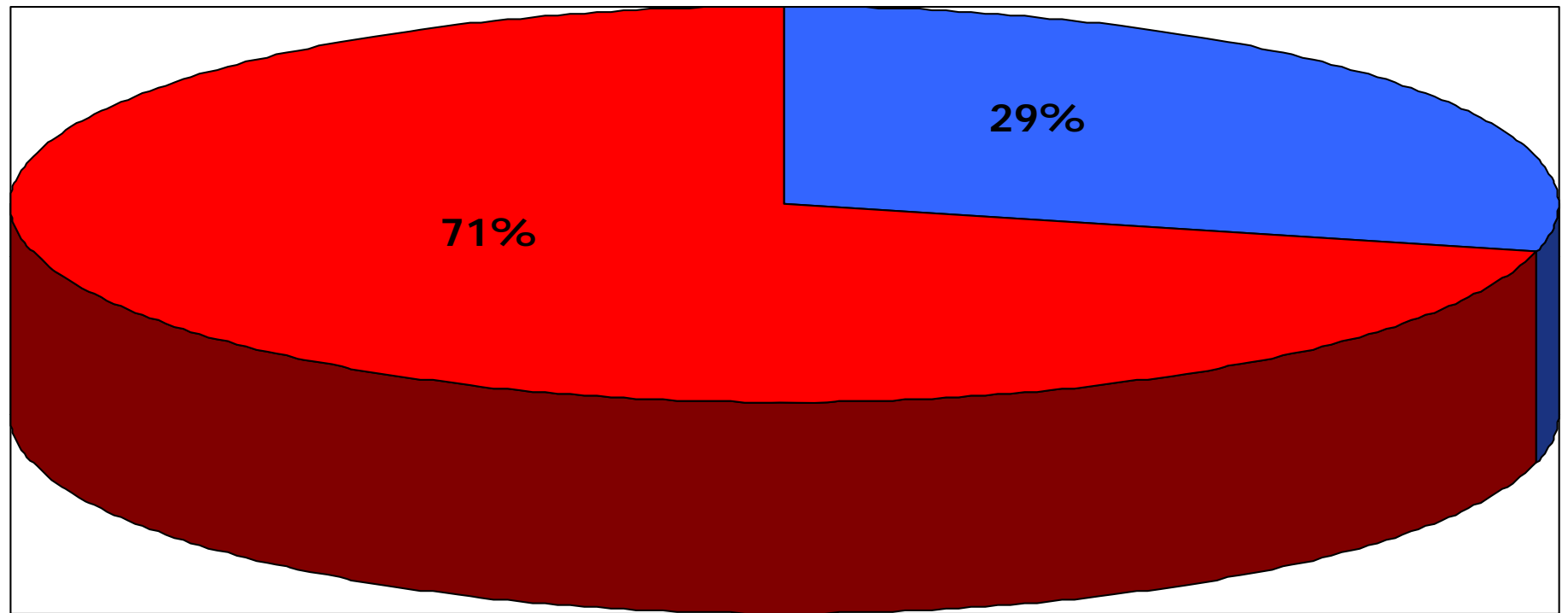
Evidence of High Focus

- Twice-yearly Self-Certifications of Compliance Status
- Required Spot-Checks in Annual CMEP Implementation Plan in 2009 and 2010
- July 2009 Supplemental Survey
- Technical Feasibility Exception Process

Transmission Owners reporting Critical Assets



Generation Owners/Operators reporting Critical Assets





Excerpt from NERC Chief Security Officer (Mike Assante) letter on 4/8/2009

“...as we consider cyber security, a host of new considerations arise. Rather than considering the unexpected failure of a digital protection and control device within a substation, for example, system planners and operators will need to consider the potential for the simultaneous manipulation of all devices in the substation or, worse yet, across multiple substations. **I have intentionally used the word “manipulate” here, as it is very important to consider the misuse, not just loss or denial, of a cyber asset and the resulting consequences,** to accurately identify CAs under this new “cyber security paradigm.”



July 2009 CIP Supplemental Survey

- July 2009 CIP supplemental surveys added to gain additional, more granular information on extent of critical asset identification
- determine total number of nuclear generating units, conventional generating stations, transmission substations, and blackstart units owned by a given entity and those that have been determined to be CA's
- NERC and Regions currently reviewing data; summary report to be presented to FERC



SERC CIP Spot Checks

- 12 CIP Spot Checks performed to date
- SERC has 30+ Table 1 entities
- SERC's Goal: Spot Check all Table 1 entities by end of 2010
- NERC has participated in 8 of the 11 spot checks
- FERC has participated in 2009
- Industry Subject Matter Expert (ISME) participation



SERC CIP Spot Check Preparation

- Auditors will look for evidence of compliance back to July 1, 2008
- Currently 13 requirements are in scope for CIP spot checks
- Evidence of training and background checks will be requested for selected employees, contractors and vendors
- Do not provide actual results of background checks, only verification that background checks were performed and the type of checks performed
- Evidence of specific access rights and the dates access rights were given and revoked will be requested for selected employees, contractors and vendors



Typical SERC CIP Spot Check Schedule

- **Day 1**

- 1:00 - 2:00 p.m. Spot Check Team meeting
- 2:00 - 2:15 p.m. SERC Opening Presentation
- 2:15 - 2:30 p.m. Registered Entity organization and computer systems presentation
- 2:30 - 3:00 p.m. Tour of computer facilities
- 3:00 - 5:00 p.m. Spot Check Team review of CIP documents

- **Day 2**

- 8:00 -12:00 p.m. Spot check interviews and discussions
- 12:00 - 1:00 p.m. Lunch
- 1:00 - 5:00 p.m. Spot check interviews and discussions
- After 5:00 p.m. Spot check team review

- **Day 3**

- 8:00 - 10:00 a.m. Final interviews and discussions
- 10:00 - 11:00 a.m. Spot check team review meeting
- 11:00 - 12:00 p.m. Exit Briefing by Spot Check Team Leader



Enforcement Process Overview

Discovery Methods

- **Self-reporting**
- Self-certification
- Compliance audits
- Spot-checks
- Periodic data submittal
- Exception reporting
- Complaints
- Compliance Violation Investigation



Enforcement Process Overview

- Discovery Methods (8)
- Compliance Assessment Notice / Initial NERC reporting
- Determination of Alleged Violation
- Penalty and Sanctions
- Pre-Notice Conference
- Notice of Alleged Violation
- Settlement/Notice of Confirmed Violation/Hearing Process
- Mitigation
- Regional Approval of Enforcement Action; Mitigation Plan
- NERC Approval of Enforcement Action; Mitigation Plan
- Notice of Penalty Filing
- FERC Acceptance/Approval



Summary Report for Possible Violations of Reliability Standard CIP-004-1

Cyber Security - Personnel & Training



CIP-004-1 Possible Violation Analysis

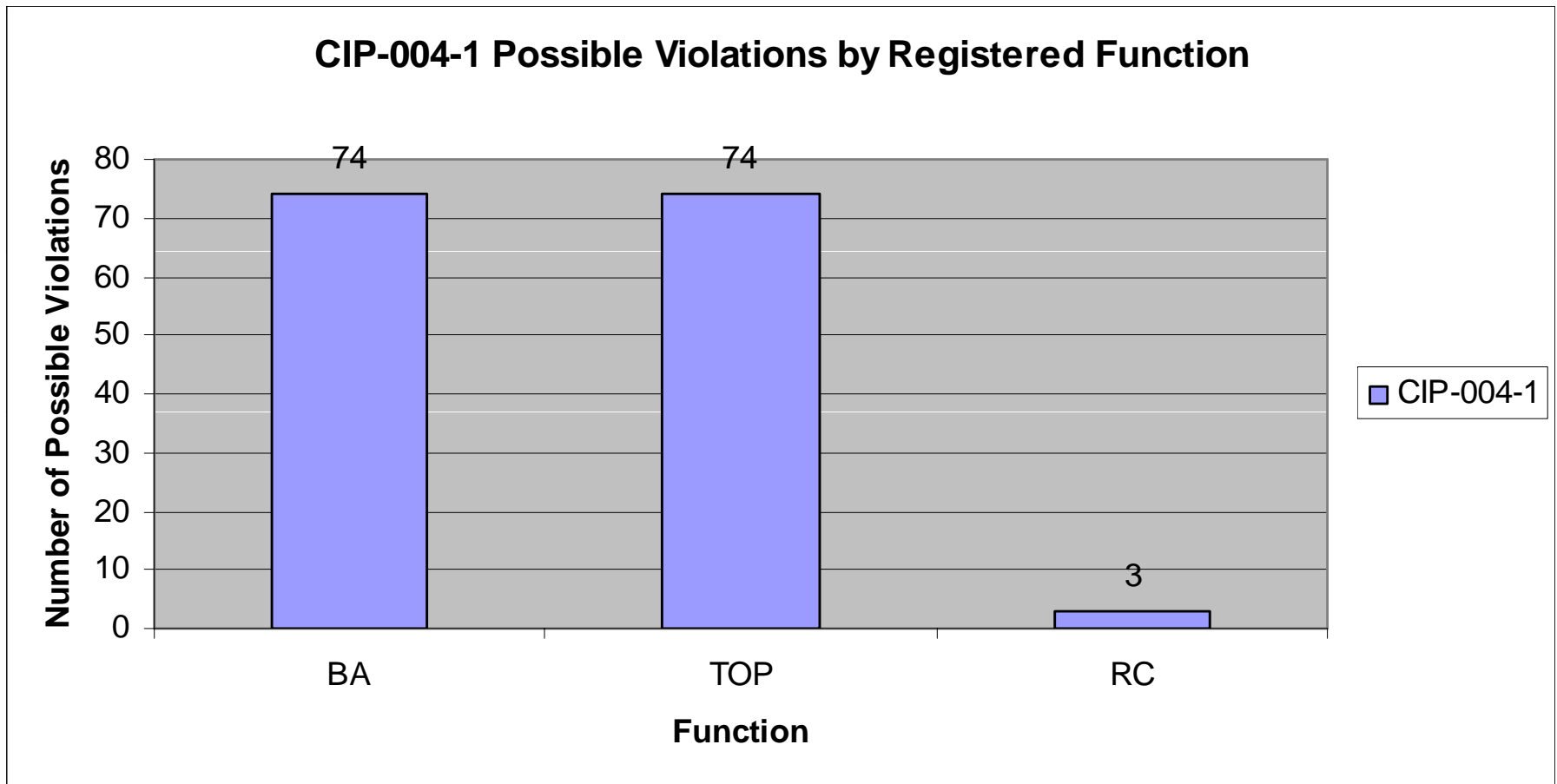
- CIP-004-1 focused on Cyber Security – Personnel and Training
- Major Requirements of this standard
 1. Awareness of Security Program
 2. Cyber Security Training
 3. Personnel Risk Assessment
 4. Personnel Access to Critical Cyber Assets



Current Possible Violation Statistics

CIP-004-1 by Requirement	Number of Violations
Requirement 1 – Awareness	0
Requirement 2 – Training	23
Requirement 3 – Risk Assessment	29
Requirement 4 – Access	28
Total	80

Possible Violations by Registered Functions

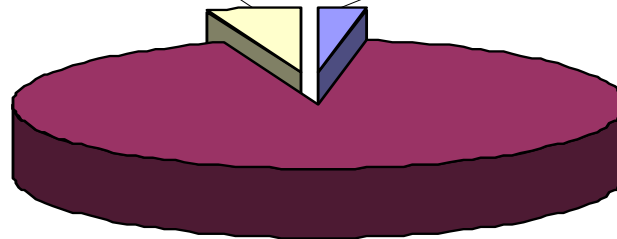


Possible Violations by Discovery Method

CIP-004-1 Possible Violations by Discovery Method

Spot Check; 4; 5%

Self-Certification; 2;
3%



Self-Report; 74; 92%

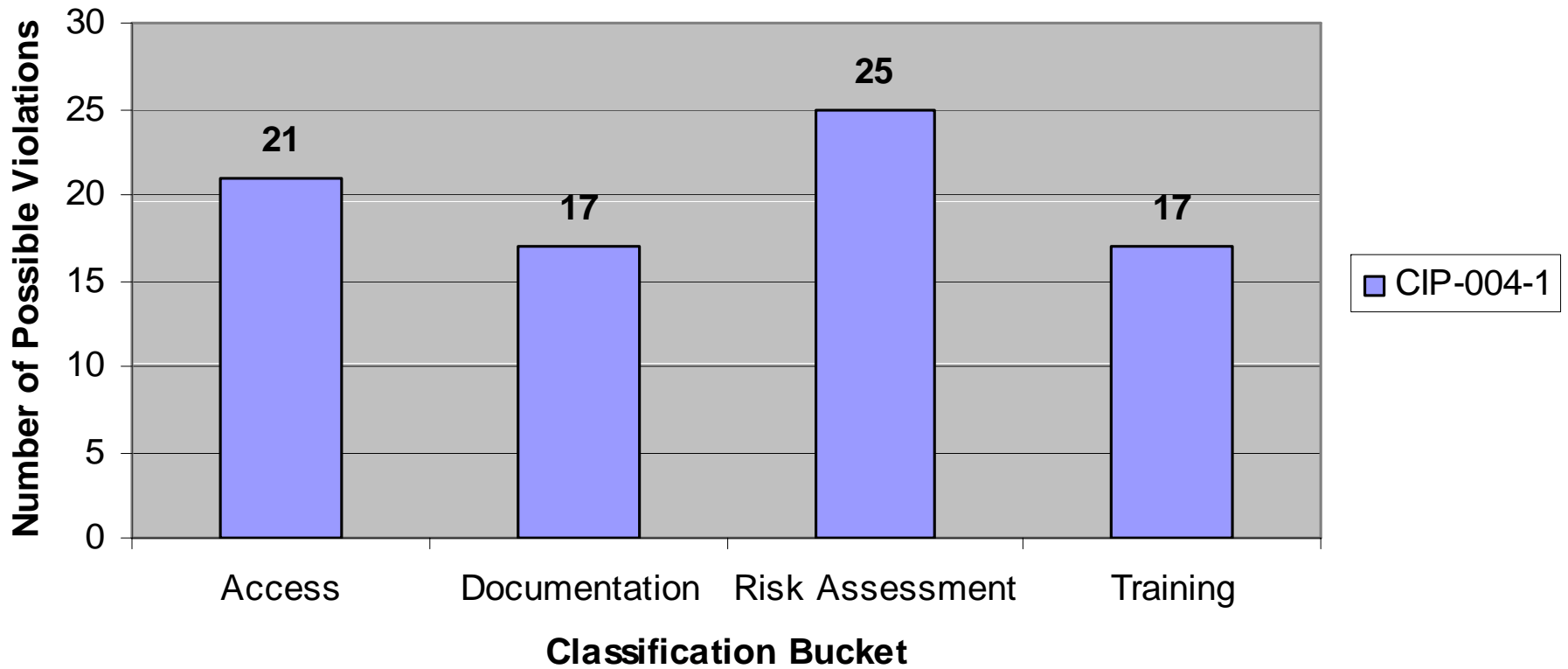


Key Reasons for Possible Violations

- Classified Possible Violations into Four Buckets
 - Documentation – a lack of Records
 - Training – training not offered / completed on time
 - Risk Assessment – background checks not complete
 - Access – granted improper access to critical cyber assets, or failed to timely revoke access

Possible Violation Buckets

CIP-004-1 Possible Violations by Classification





CIP-004-1 Lessons Learned

- Training was not completed within 90 days of being granted access, including for temporary access. (R2.1)
- Not all employees completed their annual training. (R2.3)
-



CIP-004-1 Lessons Learned

- Contractor/Vendor personnel were either not trained and/or had not had Personnel Risk Assessments within the allotted timeframes. (R2 and R3)
- Incomplete documentation of training, Personnel Risk Assessments, and dates when access was granted/revoked. (R2,R3,R4)
- Access was not removed within the required timeframes after termination or transfer of an employee. (R4.2)



CIP-004-1 Lessons Learned

- Regional Entities working on CIP-004 “White Paper” similar to PRC-005 White Paper



Regional Consistency Efforts

- Regional Compliance Implementation Group (RCIG)
- CIP Compliance Working Group (CCWG)
- Compliance Monitoring Processes Working Group (CMPWG)
- Enforcement, Sanctions and Mitigation Working Group (ESMWG)
- Registration Working Group (RWG)
- NERC-led CIP Auditor Training
- Cross-regional spot check participation and observation
- Regional Entities' Website (www.regionaleentities.org)



Questions?