

AGENDA
TECHNICAL PANEL
Varner Hall - Board Room
3835 Holdrege Street
Lincoln, Nebraska
Tuesday, September 8, 2015
9:00 a.m.

9:00 AM	<ul style="list-style-type: none"> 1. Roll Call, Meeting Notice & Open Meetings Act Information 2. Public Comment 3. Approval of Minutes* - April 14, 2015 and July 14, 2015 	Chair
9:05 AM	<ul style="list-style-type: none"> 4. Enterprise Projects <ul style="list-style-type: none"> a. Project Updates <ul style="list-style-type: none"> i. DHHS - Medicaid Eligibility & Enrollment System (EES) D. Spaulding ii. DHHS - Medicaid Management Information System (MMIS) D. Spaulding b. Project Status Dashboard A. Weekly 	
9:30 AM	<ul style="list-style-type: none"> 5. Standards and Guidelines <ul style="list-style-type: none"> a. Requests for Waiver <ul style="list-style-type: none"> i. Coordinating Commission for Postsecondary Education – Request for Waiver from the requirements of NITC 8-301: Password Standard and NITC 8-302: Identity and Access Management Standard for State Government Agencies* ii. Secretary of State – Request for Waiver from the requirements of NITC 5-101: Enterprise Content Management System for State Agencies* 	
10:00 AM	<ul style="list-style-type: none"> 6. Work Group Updates and Other Business <ul style="list-style-type: none"> a. Security Architecture Workgroup 	Chair C. Hobbs
10:15 AM	<ul style="list-style-type: none"> 7. Adjourn 	Chair

* Denotes action items.

The Technical Panel will attempt to adhere to the sequence of the published agenda, but reserves the right to adjust the order of items if necessary and may elect to take action on any of the items listed.

Meeting notice was posted to the [NITC website](#) and the [Nebraska Public Meeting Calendar](#) on August 4, 2015. The agenda was posted to the NITC website on September 3, 2015. [Nebraska Open Meetings Act](#)

TECHNICAL PANEL
Tuesday, April 14, 2015 at 9:00AM
Varner Hall - Board Room
3835 Holdrege Street
Lincoln, Nebraska
MINUTES

MEMBERS PRESENT:

Walter Weir, CIO, University of Nebraska, Chair
Jayne Scofield, State of Nebraska
Christy Horn, University of Nebraska
Kirk Langer, Lincoln Public Schools
Michael Winkle, Nebraska Educational Telecommunications

ROLL CALL, MEETING NOTICE & OPEN MEETINGS ACT INFORMATION

Mr. Weir called the meeting to order at 9:03 a.m. A quorum was present to conduct official business. The meeting notice was posted to the [NITC website](#) and [Nebraska Public Meeting Calendar](#) on February 27, 2015. The agenda was posted to the NITC website on April 10, 2015.

PUBLIC COMMENT

There was no public comment.

Approval of February 10, 2015 Minutes*

Mr. Winkle moved to approve the February 10, 2015 minutes as presented. Ms. Horn seconded. Roll call vote: Winkle-Yes, Weir-Yes, Langer-Yes, Horn-Yes, and Scofield-Yes. Results: Yes-5, No-0, Abstained-0. Motion carried.

ENTERPRISE PROJECTS

Project Status Dashboard

Project Updates, Andy Weekly. Mr. Weekly reviewed the project status dashboard report with the Panel. Members requested that the NRIN (Nebraska Regional Interoperability) project provide an in person report at the next meeting.

NEBRASKA DEPARTMENT OF EDUCATION - DISTRICT DASHBOARDS

Dean Folkers, Project Manager

Mr. Folkers was not aware that the project had not supplied a project report since December. He will follow-up on this. The project is grant funded. The vendors were responsible for the connections which put a 6-month delay on the implementation schedule. The project is a week away from implementing Parsons Power School. Infinite Campus implementation is about a month away. ESU's are currently doing pilot testing. In addition, the project is building a data warehouse to be able to move data from dashboards to centralize data. The grant will end June 30 but the agency is applying for an extension.

Panel members were given an opportunity to ask questions.

DEPARTMENT OF HEALTH & HUMAN SERVICES - MEDICAID ELIGIBILITY & ENROLLMENT SYSTEM

Eric Henrichsen, Chief Information Officer, DHHS

Mr. Henrichsen reported the following positive news:

- Progressing on the requirements phase.

- The first CMS (Center for Medicaid/Medicare Services) gate review is scheduled for June for their required deliverables. Results will have recommendations for approval.
- An integrated master schedule has been developed for current phase.
- Wipro and IBM have been working together more cohesively.

The challenges facing the project include:

- The Project Manager for Medicaid had an accident and there is no estimated time of when she will return. The project is reviewing her role and determining how to move forward.
- Project is dealing with employee morale.
- Wipro has staff in high demand and are wanted by other states.
- Although it shows under budget, extension will affect cost.
- Procurement process is lengthy and cumbersome.

Panel members were given an opportunity to ask questions.

STANDARDS AND GUIDELINES

Recommendations to the NITC

NITC 3-205: Street Centerline Standards (Amendment)*

Purpose: The purpose of this standard is to provide the necessary requirements for the creation, development, delivery, and maintenance of street centerline and address range data to support a statewide NSCD. These standards will help ensure that street centerline and address range data creation and development are current, consistent, accurate, publicly accessible, and cost effective.

NITC 3-206: Address Standards (Amendment)*

Purpose: The purpose of this standard is to provide the necessary requirements for the creation, development, delivery, and maintenance of address point data to support a statewide NAD. These standards will help ensure that address data creation and development are current, consistent, accurate, publicly accessible, and cost-effective.

Both of these standards were approved by the NITC last month but after final review, these corrections are being recommended.

Mr. Langer moved to recommend approval of the amendments to NITC 3-205: Street Centerline Standards and NITC 3-206: Address Standards. Ms. Horn seconded. Roll call vote: Winkle-Yes, Weir-Yes, Langer-Yes, Horn-Yes, and Scofield-Yes. Results: Yes-5, No-0, Abstained-0. Motion carried.

Requests for Waiver

Nebraska Tourism Commission - Request for Waiver from the requirements of NITC 7-104 (Web Domain Name Standard)*

The Nebraska Tourism Commission's website promotes Nebraska businesses and tourism attractions statewide, and includes advertisements for certain businesses and attractions. The General Services Administration's "*Gov Internet Program Guidelines*" prohibits advertisements on ".gov" domains. For this reason, the agency is requesting a waiver from using the ".gov" domain.

The Office of the CIO recommends approval of their request for waiver.

Mr. Winkle moved to approve the Nebraska Tourism Commission's request for waiver from the requirement of NITC 7-104 Web Domain Name Standard. Mr. Langer seconded. Roll call vote: Langer-Yes, Weir-Yes, Winkle-Yes, Scofield-Yes, and Horn-Yes. Results: Yes-5, No-0, Abstained-0. Motion carried.

WORK GROUP UPDATES AND OTHER BUSINESS

Other Business

Members discussed the new state IT spending initiative and the University's data center option for the future.

ADJOURNMENT

Ms. Horn moved to adjourn the meeting. Mr. Langer seconded. All were in favor. Motion carried.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by Rick Becker of the Office of the CIO.

TECHNICAL PANEL
Tuesday, July 14, 2015 at 9:00AM
Varner Hall - Board Room
3835 Holdrege Street, Lincoln, NE
MINUTES

MEMBERS PRESENT:

Walter Weir, CIO, University of Nebraska, Chair
Ed Toner, CIO, State of Nebraska
Michael Winkle, Nebraska Educational Telecommunications

MEMBERS ABSENT: Christy Horn, University of Nebraska and Kirk Langer, Lincoln Public Schools

ROLL CALL, MEETING NOTICE & OPEN MEETINGS ACT INFORMATION

Mr. Weir called the meeting to order. A quorum was present to conduct official business. The public meeting notice was posted to the [NITC website](#) and [Nebraska Public Meeting Calendar](#) on June 4, 2015. The agenda was posted to the NITC website on July 10, 2015. [Nebraska Open Meetings Act.](#)

PUBLIC COMMENT

There was no public comment.

ENTERPRISE PROJECTS

Project Updates

NEMA - Nebraska Regional Interoperability Network (NRIN)

Sue Krogman, Nebraska Information Management Agency

The original contract was cancelled. The Office of the CIO had a master service agreements with two contractors. NEMA was able to use these agreements for the grant year. The grant closed in March 2015. A deviation contract for continuation was submitted to the Department of Administrative Services. It was approved. There are different levels of completion at over 100 sites. There is an estimated \$1.8 million left for the project. The project is scheduled for completion by the fall of 2016. All systems run on redundant rings. The Public Safety Statewide Radio System will be backup for NRIN and vice versa. Sustainability after completion is being discussed. Discussions have occurred with Lt. Governor and Governor. The Governance Board will include NACO and local entities that own the site. Local jurisdictions will need to look at federal requirements. Each region will have spare parts available to them for immediate fixes. The Office of the CIO monitors two of the regions. There are MOU's with the involved regions.

DHHS - Medicaid Eligibility & Enrollment System

Eric Henrichsen, CIO, Health and Human Services

Mr. Henrichsen provided an update to the Panel. There is a revised end date -- 1st quarter of 2017. The first GAT review will be occurring soon. So far, 14 deliverables have been approved and Wipro will be paid for these. First Data Government Solutions will be doing the IV&V for CMS. The project is 90% federally funded. Members discussed the hosting arrangement for the appliance and related costs.

Project Closure

Administrative Services - LINK-Procurement*

Members requested that the project manager report to the Panel at the next meeting. The Panel will consider recommending closure of the project after receiving that report.

[Project Status Dashboard](#)
Andy Weekly

Mr. Weekly reviewed the project status dashboard.

STANDARDS AND GUIDELINES

Request for Waiver

DHHS - [Request for Waiver](#) from the requirements of [NITC 8-302](#): Identity and Access Management Standard for State Government Agencies*

Chris Hobbs, State Security Officer

The agency wants to use the DHHS Active Directory rather than the OCIO Active Directory for this application. Discussion occurred regarding directory services for the State of Nebraska. Mr. Weir recommended that the State and the University meet to discuss shared interests. Mr. Weir invited members to attend the University security meeting held every Thursday, 10:15 a.m.

Mr. Winkle moved to approve the Department of Health and Human Services waiver request with a sunset date of June 30, 2016. Roll call vote: Toner-Yes, Weir-Yes, and Winkle-Yes. Results: Yes-3, No-0, Abstained-0. Motion carried.

WORK GROUP UPDATES AND OTHER BUSINESS

Security Architecture Workgroup Update - Chris Hobbs

Mr. Hobbs provided an update on the activity of the Workgroup. The Workgroup has been reviewing issues related to PII. The Workgroup also performed a gap analysis of the NITC Standards & Guideline and determined they are in need of an update.

Mr. Weir and Mr. Toner would like to have further discussions regarding cloud computing, cloud environments, services platform and software in regards to cost effectiveness.

ADJOURN

Mr. Winkle moved to adjourn. All were in favor. Motion carried.

The meeting was adjourned at 10:20 a.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by Rick Becker, Office of the CIO.



TO: NITC Technical Panel

FROM: Gary Timm, CFO
Coordinating Commission for Postsecondary Education
Gary.Timm@nebraska.gov
402.471.0020

DATE: August 12, 2015

RE: Request for Waiver

NITC Standards and Guidelines:

NITC 8-301: Password Standard

NITC 8-302: Identity and Access Management Standard for State Government Agencies

Description of problem or issue

The Commission and OCIO are in the process of testing and deploying tracking software that will be used by high school guidance counselors to identify the completion status of their high school students Free Application for Federal Student Aid (FAFSA). Through this application, the guidance counselors will have access to Personally Identifiable Information in the form of the student's name, school district, student's state ID, date of birth, and whether the FAFSA has been completed for only students in their school system. With the exception of the stage of the FAFSA completion, this information is considered directory information for the high school under the Family Educational Rights and Privacy Act (FERPA) and schools may disclose this information without consent. Additionally, the guidance counselors would already have access to the directory information through their duties with the high school and will have provided this information to the Commission. The Commission's intent is to make this tool available during September 2015.

Per NITC 1-103, the Commission is requesting a waiver of NITC 8-301: Password Standard. The Commission and the OCIO are in the process of implementing a third-party web application with a built-in authentication process. While various parameters of the password construction can be set within the application that allows the commission to meet NITC 8-301, section 1.2 Minimum Password Complexity Construction, there is no provision requiring the expiration of passwords as required for confidential information under section 2.2.

In addition, the Commission is requesting a waiver of NITC 8-302: Identity and Access Management Standard for State Government Agencies. While this software has the capability to authenticate using social media userid/passwords, which will not be allowed by the Commission, no provision has been included in the code to allow for authentication required under NITC 8-302. The Commission is working with the developer to provide a solution that would allow this type of authentication.

Commissioners

Colleen A. Adam, Chair
Hastings

Carol Zink, Vice Chair
Lincoln

Dr. John Bernthal
Lincoln

Dr. Deborah Frison
Omaha

Dr. Ron Hunter
Hay Springs

Mary Lauritzen
West Point

Dwayne Probyn
Papillion

Eric Seacrest
North Platte

Dr. Joyce D. Simmons
Valentine

Lori Warner
South Sioux City

W. Scott Wilson
Papillion

Description of agency's preferred solution

The Commission is in the process of relocating its in-house data and web applications to the OCIO. As this project progresses, the Commission will be coordinating an authentication solution for all applications that meets both NITC 8-301 and NITC 8-302. Until this time, the Commission requests a waiver to utilize the user authentication processes included in the FAFSA software. The Commission's intent is to be able to meet both NITC 8-301 and NITC 8-302 by June 30, 2016.

Additional information

Some types of financial aid are awarded on a first-come first-serve basis. Many colleges set priority dates in February or March. Students whose FAFSAs are submitted by the priority dates are then eligible to be considered for these limited aid options. Implementing this software in September will provide the high school guidance counselors time to provide the Commission with a listing of students that will be graduating in May 2016 and for the Commission to provide FAFSA completion data back to them by the February/March 2016 priority dates.

NITC 8-301: Password Standard

Category: Security Architecture

Applicability: Applies to all state agencies, boards, and commissions, excluding higher education

History: Adopted on September 18, 2007. Amended on November 12, 2008 and December 10, 2013.

1. Purpose

The purpose of this standard is to set the minimum requirements for passwords and the related system access requirements based on the data classification (NITC 8-101, § 4.6).

1.1 Scope

The scope of this standard is restricted to passwords that are used to authenticate users to networks or applications.

1.2 Minimum Password Complexity Construction

The following are the minimum password requirements for State of Nebraska passwords:

- Must contain a minimum 8 characters
- Must contain at least three (3) of the following four (4):
- At least one (1) uppercase character
- At least one (1) lowercase character
- At least one (1) numeric character
- At least one (1) symbol
- Cannot repeat any of the passwords used during the previous 365 days.

2. Standard

In addition to the Minimum Password Complexity outlined in section 1.2, additional password requirements are necessary for differing levels of data classification when authenticating users to networks or applications. The highest data classification level that a user has access to during an authenticated session will determine the additional password requirements. All employees and contractors of the State of Nebraska shall use a password that follows at least a confidential level of authentication when logging into a state network or application.

2.1 Highly Restricted

Information that is deemed highly restricted requires the highest level of security. A password used to access Highly Restricted information must follow the password complexity rules outlined in section 1.2 and must contain at least 2 of the following additional requirements:

- Multi-factor authentication
- Expire after 60 days
- Minimum Password Age set to 15 days

2.2 Confidential

Information that is deemed Confidential requires a high level of security. A password used to access Confidential information must follow the password complexity rules outlined in section 1.2 and must contain the following additional requirement:

- Expire after 90 days

2.3 Managed Access Public

Information that is deemed Managed Access Public requires minimal level of security and need not comply with section 1.2 of this policy. Typically this data would not include personal information but may carry special

regulations related to its use or dissemination. Managed Access Public data may also be data that is sold as a product or service to users that have subscribed to a service.

2.4 Public

Information that is deemed Public requires no security and need not comply with section 1.2 of this policy. This information should be restricted to view only.

3. Non-Expiring Passwords

Non-expiring passwords require a unique high level of security. Typically this information is confidential in nature and must follow the requirements in section 1.2. The additional requirements for access to confidential data with a non-expiring password are:

- Must contain at least one of the following additional security features:
- Extended password length to 10 characters
- Personal security question may be asked
- Multi-factor authentication
- Any feature not included on this list may also be utilized upon approval of the State Information Security Officer or upon enactment of federal, state or departmental laws, policies or directives.

3.1 Automated System Accounts

Agencies may use non-expiring passwords for automated system accounts. Examples of automated system accounts include those that act as an intermediary between the public user and state systems, internal system to system interfaces, perform backups or run batch jobs.

3.2 Multi-user Computers

Agencies may use non-expiring passwords on multi-user computers. Examples of multi-user computers include those computers in kiosks or training labs, where users have limited or restricted access to state resources.

3.3 System Equipment/Devices

Agencies may use non-expiring passwords for system equipment/devices. It is common for many devices (e.g. IP cameras, HVAC controls) in today's IT environment to utilize login capabilities to protect the device from unauthorized access. While many of these devices make use of a user ID and password in a manner similar to those found while authenticating a user, the distinction to be made is that the User ID is used to authenticate the device itself to the system and not a person.

NITC 8-302: Identity and Access Management Standard for State Government Agencies

Category: Security Architecture

Applicability: Applies to all state agencies, boards, and commissions, excluding higher education

History: Adopted on March 15, 2005. Amended on March 4, 2008 (by NITC 1-103).

1. Standard

All state government web applications that require authentication and authorization of users will utilize the enterprise directory, known as Nebraska Directory Services.

2. Purpose and Objectives

The purpose of this standard is to provide an enterprise solution for identity and access management capabilities to reduce security administration costs, ensure regulatory compliance, and increase operation efficiency and effectiveness. This standard focuses on web applications, because most if not all new applications will utilize web technology. To incorporate non-web applications into the Nebraska Directory Services would require additional cost and different policies to implement.

Objectives include:

- Build an identity-based portal that can integrate disparate applications, enable secure web access to applications and data, and enable users to access applications from their offices or remote locations.
- Implement a standardized, secure identify and access management architecture that provides centralized management with local administration of users, centralized user identity information, synchronized user identity information across multiple applications (where appropriate), and application-level authentication and authorization based on the unique identity of the user (as opposed to a shared logon ID).
- Use standards-based technology to ease application integration, provide for reuse of components and remain adaptable in the face of changing technology products.
- Ensure a solution that is scalable to meet the current and future needs of state agencies, their employees, clients and customers, and business partners.
- Meet federal security requirements for identity and access management, including HIPAA and NCIC security regulations.
- Provide a high level of security including the option of two-factor identification.

3. Definitions

Authentication: The process of uniquely identifying an individual. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Authorization: The process of giving individuals access to system objects based on their identity which allows them to add, update, delete or view information for a web application.

Identify and Access Management: Enterprise Identity Management is a system of technologies, business practices, laws and policies that manages common identification of user objects; reduce the costs while enhancing the quality of government services; protects the integrity of state resources; and safeguards the privacy of the individual.

LDAP: LDAP (Lightweight Directory Access Protocol) is an Internet protocol that applications use to look up user information from a server, such as Novell's eDirectory.

Web Applications: Web server based applications that are accessed using a web browser. This definition includes custom developed systems and third party software systems.

4. Applicability

4.1 State Government Agencies

This standard applies to all state government agencies, boards, and commissions, except Higher Education.

4.1.1 State Agencies, Boards, and Commissions

All new web applications requiring authentication and authorization of individuals must comply with the standard listed in Section 1. All existing web applications requiring authentication and authorization must convert to the standard listed in Section 1 as soon as fiscally prudent or upon an upgrade to the web application, whichever comes first, unless the application is exempt.

5. Responsibility

5.1 IMServices

IMServices will incorporate the needed hardware and software into their infrastructure to provide the following:

- LDAP directory for user /entity objects.
- Role-based authentication and authorization to the enterprise LDAP directory and applicable applications for registered users.
- Business/disaster recovery.
- Authentication methods available:
- User ID and password
- Two-factor authentication
- X.509 certificates

5.2 State Agencies, Boards and Commissions

Agencies, Boards and Commissions will carry out the following responsibilities:

- Web applications requiring authentication and authorization must comply with the standard listed in Section 1.
- Require this standard be referenced in all RFPs (Requests for Purchase) for web applications covered by this standard.

5.3 State Government Council Directory Services Workgroup

The State Government Council's Directory Services Workgroup will provide ongoing advice and direction, including but not limited to:

- Policies for implementation;
- Benchmarks and service level agreements;
- Funding options.

Request for Waiver of NITC Standard 5-101

Agency name:

Nebraska Secretary of State

Contact information:

Colleen Byelick
1445 K Street, Suite 2300
Lincoln, NE 68509
PH: 402-471-8076
colleen.byelick@nebraska.gov

Title of the NITC Standards and Guidelines document at issue:

NITC 5-101 Enterprise Content Management System for State Agencies

Description of the problem or issue:

The Business Services division of the Office of the Secretary of State is replacing a legacy corporate and UCC filing system and is currently in the RFP drafting stage of the project.

The existing legacy filing system interfaces with an OnBase image library to retrieve and maintain images of filed corporate and UCC documents.

In reviewing replacement systems, we have learned many contain an image library which is native to the filing system software.

The office desires to write the RFP for the filing system to solicit dual responses from vendors regarding the image library component as follows: (1) efficiencies and image conversion costs associated with using the native image library and (2) costs associated with integrating the filing system software with the OnBase image library and any loss of functionality associated with using the OnBase library.

Description of the agency's preferred solution, including a listing of the specific requirement(s) for which a waiver is requested:

The office seeks a waiver of NITC standard 5-101 Enterprise Content Management Systems should the agency determine that it is more efficient or economical to utilize the filing software's native image library.

Any additional information and justification showing good cause for the requested waiver:

We believe there may be enhanced efficiencies and functionality available by utilizing the image library native to these types of filing systems. However, until formal bids are received, reviewed

and evaluated, we will not have comparative information available to present to the Commission. Once the evaluation process is complete and should our agency determine that it is more efficient or economical to utilize the filing software's native image library, those findings would be presented to the NITC at that time.

NITC 5-101: Enterprise Content Management System for State Agencies

Category: Groupware Architecture

Applicability: Standard for all State government agencies, excluding higher education

History: Adopted on April 11, 2012.

1. Standard

1.1

State agencies managing content and creating workflow as described in Section 2 shall use the Enterprise Content Management System (ECM) that is provided through the Office of Chief Information Officer (OCIO).

1.2

Agencies must consider, through consultation with the OCIO, using the ECM's E-Forms software for any new electronic forms applications.

2. Managing content and creating workflow includes the following

- Capturing paper documents through the use of scanners and storing them in electronic form;
- Capturing all type of content (audio, video, e-faxes, emails, MS Office documents, etc) and storing them in electronic form;
- Electronic searching and retrieval of captured content;
- Automating records retention and archiving;
- Automating business processes through workflow;
- Reducing and/or eliminating paper document storage.

3. Purpose

The purpose of this standard is to provide, to the extent possible, a single technical solution for State agencies:

- Capturing all types of content and storing content electronically;
- Converting and minimizing the number of paper documents the State maintains;
- Facilitate searching and retrieval of electronic documents;
- Retain and dispose of electronic documents based on established document retention policies;
- Improve efficiency and accuracy of exchanging information; and
- Unify document management in a single system to take advantage of economies of scale.

4. Exception

This standard does not apply to systems already in use by an agency, unless:

- The agency intends to buy significant upgrades;
- The agency intends to buy a significant amount of new modules; or
- The agency intends to do a significant amount of custom development

For guidance on these points, contact the OCIO.

5. Definitions

Documents: The State currently utilizes a great deal of paper-based documents. These documents are generated internally from both manual and automated processes. Paper documents also come from external businesses and citizens. Additionally, each paper document is read by a person to determine its purpose, what information it contains, what it is associated with and what should be done with it.

Indexing is a process of extracting the key content of the document and storing that information with the electronic version of the document. The purpose of the index information is to facilitate searching and retrieval of the document and facilitate automating processes using workflow in an agency. The index information can also be used for securing the document as well as to associate multiple documents together.

The ECM will consume paper documents by either using scanners and/or electronic document uploads. The documents can be indexed by automated means using Optical Character Recognition (OCR), Intelligent Character Recognition (ICR) and/or bar codes. The ECM facilitates both automated and manual indexing.

Processes (Workflow): For those paper documents that are processed manually, (i.e. from one desk to another, one agency to another, and are dependent on individual organizational skill sets to insure documents are not lost, processed timely, processed accurately and filed correctly) can be greatly improved with automated workflow. Even automated processes that were previous built with little or no integration to other processes can be improved and enhanced as well.

The ECM supplies a framework to allow agencies to easily create flexible automated workflows that can utilize documents or work as independent processes. These automated workflows readily integrate with existing processes.