

24.0 System Security & Authority Process Report

March 2018



Copyright

Copyright © 2018 University of Illinois – Office of Business and Financial Services. All rights reserved. No part of this publication may be reproduced or used in any form or by any means—graphic, electronic or mechanical, including photocopying, recording, taping or in information storage and retrieval systems—without written permission of University of Illinois – OBFS.

APPROPRIATE USE AND SECURITY OF CONFIDENTIAL AND SENSITIVE INFORMATION

Your responsibilities regarding the protection and security of administrative information are outlined in the University of Illinois Information Security Policy for Administrative Information and Guidelines posted at https://www.aitis.uillinois.edu/reference_library/i_t_policies. Any violation could subject you to disciplinary action, which could include dismissal or, in those cases where laws have been broken, legal action. You should have signed a compliance form that indicates you have read, understand and agree to comply with the University's Information Security Policy for Administrative Information. If you have not already signed the compliance form, please see your Unit Security Contact, who is responsible for maintaining these forms.


TABLE OF CONTENTS

Overview	1
Process Executive Summary	2
Chapter 1: SIPOC Diagram.....	4
Chapter 2: Suppliers	5
AITS –Enterprise System Coordination Finance	5
AITS –System Access Management	5
Authorizer Group	5
Sec App	5
Service Desk Manager	5
University Department Unit/Employee.....	5
Unit Security Contact (USC)	6
Business Rules	6
Chapter 3: Inputs.....	7
Approvals	7
Basic user information	7
Request for new/updates to access	7
Business Rules	8
Chapter 4: Process	9
Identify need for new/update access	9
Grant/reject access reject	9
Finalize access	9
Business Rules	10
Chapter 5: Outputs.....	11
Access to a system application	11
Response to requestor	11
Denial of access and reason	11
Terminated access	11
Business Rules	11
Chapter 6: Customers.....	12
University Department Unit/Employee.....	12
University Contract Records Office (UCRO)	12
Unit Security Contact (USC)	12
Business Rules	12
Chapter 7: Customer - Oversight Roles.....	13
Auditors – Internal and External	13
Board of Trustees	13
Legislature	13
AITS Enterprise System Assurance	13
Business Rules	13

Chapter 8: Questionnaire for Current State Analysis	14
Chapter 9: Questionnaire for Potential Process Improvement Candidates.....	17
Chapter 10: Current State Metrics	18
Chapter 11: Feedback from Customer Focus Groups – Current State	19
Chapter 12: Opportunities for Improvements	20
Chapter 13: Suggested Improvements	23
Chapter 14: Feedback from Customer Focus Groups – Future State	24
Chapter 15: Recommendations for Improvements	26
Chapter 16: Solutions Prioritization Matrix	30
Chapter 17: Future State SIPOC Diagram.....	32
Chapter 18: Future State Requirements	33
Chapter 19: Subject Matter Expert Team	34
Chapter 20: University Focus Group Participants.....	35
Appendix A: Business Glossary	36

Overview

This report contains the process System Security Authority. It documents providing access to applications supported by Purchasing and Procurement Services which allow authorized employees the tools to perform their job duties.

Illinois Mandate Symbol - 

University Policy Symbol - 

Professional Mandate Symbol - 

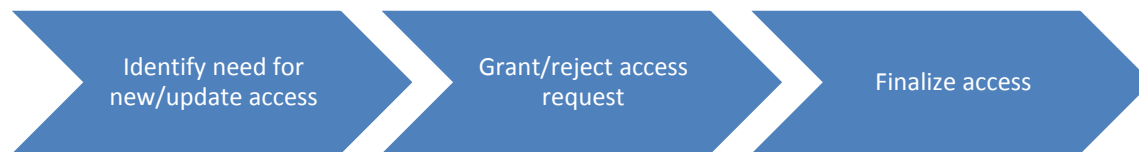
Process Executive Summary

Business Process

The process System Security Authority is used to provide access to applications supported by Purchasing and Procurement Services. The process begins when a need has been identified to access a Purchasing or Procurement Services' application(s).

When access is needed for a Purchasing or Procurement Services application, an employee's manager will submit a request to the Unit Security Contact (USC) who will review the request and submit for processing. If additional approval is needed, the request is routed for approval. If the request is rejected, the reason for reject is sent to the USC and the employee. A request can be for a new employee profile, a changes to an existing profile or a separation of employee profile.

Current Process Activities



Approach

The current state process activities were mapped by the Subject Matter Expert (SME) and project process team. A SIPOC diagram was created to capture the tasks executed by the University System departments. The SME project team identified opportunities for improvement and brainstormed potential solutions. The current state was presented, issues were identified, and recommendations were discussed at customer focus group meetings in the University System. The process report was presented to the Source2Pay Director Council where they ranked the proposed recommendations for implementation.

Key Findings

- Lack of knowing what access exists for applications supported by Purchasing and Procurement Services
- Lacking of knowing how to request access for the applications supported by Purchasing and Procurement Services
- Lack of understanding the workflow to process the access request, and the amount of time it takes to complete the granting of the access request.
- Lack of documentation
- Lack of an automated system to grant access

Improvement Recommendations

The process team identified eight suggested improvements, and from the suggested improvements the team selected six recommendations for implementation. The Director Council reviewed the six recommendations and ranked the proposed recommendations for implementation.

Listed are the top four recommendations for implementation:

24.0 System Security Authority

1. Provide a list of available access profiles for the applications Procurement Services and Purchasing provide support to
2. Provide system notifications when access has been granted to the applications Procurement Service and Purchasing provided support to.
3. Create a visual workflow to communicate the timeline to create/grant access to the Procurement Services and Purchasing applications.
4. Create a project to capture and document the process and procedures for off-boarding of a Procurement Services and Purchasing applications.

Chapter 1: SIPOC Diagram

Process Name	Date
24.0 System Security Authority Current State	January 2018

SUPPLIERS	INPUTS	PROCESS	OUTPUTS	CUSTOMERS
<u>Who</u> provides input to the process	<u>What</u> goes into the process	<u>How</u> the inputs are transformed to outputs	<u>What</u> comes out of the process	<u>Who</u> received the outputs of the process
AITS – Enterprise System Coordination - Finance AITS - System Access Management Authorizer Group Sec App Service Desk Manager University Department Unit/Employee USC	Approval from data managers Basic User information Request for new/update to access	Identify need for new/update access Grant/reject access request Finalize access	Access to a system application Response to the requestor Denial of access and reason Terminated access	UCRO University Department Unit/Employee USC

Chapter 2: Suppliers

Suppliers provide input to the process:

AIMS –Enterprise System Coordination Finance

What they care about: Making sure all approvals have been obtained for each access request, and proper access is granted to the user

When they care: When a request for access is submitted

AIMS –System Access Management

What they care about: Making sure all approvals have been obtained for each access request, and proper access is granted to the user

When they care: When a request for access is submitted

Authorizer Group

What they care about: The reason the user is requesting access; the supporting authorization; and if applicable, the user has been trained to use the system application

When they care: When the request for access is submitted

Sec App

What they care about: when the application is available for use

When they care: when a user needs to use the application

Service Desk Manager

What they care about: when the application is available for use

When they care: when a user needs to use the application

University Department Unit/Employee

What they care about: Getting access to purchasing and procurement services' application(s) to do their job

When they care: When they request access, and when they start a new role

Unit Security Contact (USC)

What they care about: Having all the information needed within a submitted request; conflicting roles with current users have been resolved; the request for access is coming from a manager and not directly from the employee; and the actual request has been submitted and received

When they care: When the request comes in

Business Rules

Employees must complete training in iCS

Chapter 3: Inputs

Inputs are information or verification which goes into the process

Approvals

Basic user information

- Name
- Phone number
- UIN/NET ID
- University email address

Request for new/updates to access

- Authority Application
- Banner
 - Approver queue
 - Chart and Org(s)
 - Dollar limit range
 - Profile
 - Role
- iBuy
 - Approver queue
 - Chart and Org(s)
 - Dollar limit range
 - Profile
 - Role
- iCS
 - Chart and Org(s)
 - Authority level (requestor, Dean/Director, unit head and business manager)
- Name
- Net ID
- Phone
- SecApp
- TEM

- UIN
- University email address
- Work address

Business Rules

Applications

- Email must be a university email and phone

Chapter 4: Process

A process is defined as the method for transforming inputs into outputs:



Identify need for new/update access

When a new University/System employee or an existing employee identifies a need to access a system application that Purchasing or Procurement Services supports, along with access for Purchasing and Procurement Services' staff a request for access is submitted. The employee's manager or a department's internal IT department submits the request to the Unit Security Contract (USC) requesting an update to the access in the system application.

An update to access would include:

- New employee profile
- Change to existing employee profile
- Separating of employee profile

System applications include:

- Banner
- iBuy
- iCS (Procurement Contracts Only)
- PCS (P-Card Web Solutions software)
- TCS (T-Card Solutions software)
- TEM

Grant/reject access reject

Once the request for access is received by the USC, information such as: Name, UIN/NET ID, University Email address, application, role, and Chart/Orgs are reviewed for completeness; reviewed for segregation of duties; and reason for request. If the information is incomplete, the USC will return the request to the employee's manager for additional information. Depending on the application's business rules additional approval may be needed from the Application's Authorizer Group. Once complete information and authorization has been provided the request is processed. If the request is denied, the reason for reject is entered into the SecApp Application, a notification is sent to the USC and requesting employee.

Finalize access

The USC and/or the end user will receive a manual email notification when access has been granted to iBuy and iCS. In some instances a manual email will be sent to advise access to Banner or TEM has been granted.

Business Rules

Employees must complete training within the iCS application prior to authority being granted.

Chapter 5: Outputs

Outputs are the resulting information or entities that are produced as part of the process:

Access to a system application

Response to requestor

Denial of access and reason

Terminated access

Business Rules

None applicable

Chapter 6: Customers

Customers receive the output of the process.

University Department Unit/Employee

What they want: Access to Purchasing and Procurement Services' system applications to allow an employee to perform their job duties

University Contract Records Office (UCRO)

What they want: Employee's profile setup within the iCS application

Unit Security Contact (USC)

What they want: to grant system application access to complete the access request

Business Rules

None applicable

Chapter 7: Customer - Oversight Roles

Customers who provide oversight and what oversight is needed: (Example Funders, OBFS, Auditors, Board of Trustees (BOT), Legislature, Public)

Auditors – Internal and External

What they want: Make sure everything is getting setup and there are segregation of duties

Board of Trustees

What they want: Properly granted access to Systems Security. The Board of Trustees owns the iCS system, and is concerned who has access to University Contracts. The Board of Trustees also have contracts with financial institutions.

Legislature

What they want: compliance with Procurement policies

ITS Enterprise System Assurance

What they want: approved access granted to employee to perform their duties

Business Rules

None applicable

Chapter 8: Questionnaire for Current State Analysis

1. Why does the process exist?

Because people need or require access or changes to systems

Provide access to applications supported by Purchasing and Procurement Services which allow authorized employees the tools to perform their job duties

2. What is the purpose of the process?

Protection of data and access limited to authorized users.

Grant staff access to correct tools to perform their job.

3. What are the process boundaries (i.e., when does it start and end?)

The process starts when a need has been identified to access a Purchasing or Procurement Services application(s)

The process ends when the request has been granted or the request has been denied with a reason provided.

4. What are the major activities/steps in the process?

See [Chapter 4: Process](#) (Ctrl-click to follow link)

5. What is the expected outcome or output of the process?

See [Chapter 5: Outputs](#) (Ctrl-click to follow link)

6. Who uses the output of the process, and why?

See [Chapter 6: Customers](#) (Ctrl-click to follow link)

7. Who benefits from the process, and how?

Employees – gaining access to the tools to do their job

University – only people having access to system applications have access

8. What information is necessary for the process?

See [Chapter 3: Inputs](#) (Ctrl-click to follow link)

9. Where does that information come from?

See [Chapter 2: Suppliers](#) (Ctrl-click to follow link)

10. What effect does that information have on the process and output?

Information is needed to perform the process and produce the outputs, users are not able to perform their jobs without access to system applications.

11. Who is primarily responsible for the process?

- AITS ESC Finance
- AITS Systems Access Management
- Department Supervisors
- UCRO
- USC

12. What other units/organizations participate in or support the process?

- Auditors (internal and external)
- Contract processing officers at each University

- TAM Finance

13. What Information Technology system(s) support the process?

- Authority
- Banner
- Email
- iBuy
- iCS
- SecApp
- Service Desk Manger
- TEM

14. What policies guide or constrain the process?

Limitations to access only to systems and data that are related to the person's position

Separation of Duties example cannot request system access for self

15. How often does the process get executed?

Multiple times per day, currently, there is a process runs twice daily to list the request for access for the iBuy and iCS applications.

Number of update generated out of the AITS Security Application by USCs from January 2017 – December 2017

<i>Application</i>	<i>Number of request</i>
iBuy	1,850
iCS	159
TEM	9,975

16. What are potential defects with respect to the process?

- Off-boarding is not happening as it should
- Conflicting actions between old and new USCs when employee changes jobs, example of issue may have access removed by the old USC that was just granted by the new USC for the new job role
- Lack of "Access Profiles" that specify what access each position should be given. This complicates employee onboarding and off boarding process, example job descriptions are very broad
- Employee off boarding sometimes leaves items in workflows that are no longer assigned to anyone, or still assigned to the person that has left the position
- Manual process to inactivate all access, and no centralized location to know what access exists
- Human error

a. How often do the potential defects occur? Multiple times per day

17. What types of challenges have employees who participate in the process raised?

- Lack of understanding of what access should be requested
- How to request the access

24.0 System Security Authority

- Lack of documentation
- Time involved in getting a new employee configured accurately
- Lack of clarity as to what happens once request is submitted, example: need a queue to view the status of the request

18. What types of challenges or concerns have customers raised?

- Lack of understanding of what access should be requested
- How to request the access
- Lack of documentation
- Time involved in getting a new employee configured accurately
- Lack of clarity as to what happens once request is submitted, example: need a queue to view the status of the request

19. Will the process be changed by another initiative in the near future?

None at this time

Chapter 9: Questionnaire for Potential Process Improvement Candidates

1. How would the process operate differently in the “Perfect Situation?”

- Having a one stop shop to request all the access that we need, one website and enter all the information into a workflow to be routed to receive the proper approvals.
- Would like to have security set up by roles instead of by person or customized roles for USCs to select.
- Automated notification or status of your request at all times

2. What does the team hope to achieve through this improvement?

- Less databases and systems to manage and use
- Time savings, visibility to know status of request, and transparency
- Prevents conflicting roles from occurring
- User friendly – very intuitive, clear instructions and process, and an overview of how it all works
- Prompts or wizards to help the user through the process

3. Who would benefit from the desired improvement to the process?

- AITS Security
- Employees
- University Department
- University Department Business Managers
- USCs

a. How would we know?

Staff would spend less time looking for status, reducing emails, save money by not having to have as many employees doing the work and in the time savings throughout the process. And happier personnel.

4. What data can be provided with respect to the process performance (e.g. service rating, cycle time, customer survey responses, etc.)?

- Processing time/cycle times
- Service desk tickets (start to finish)

5. Who should be included in any improvement discussions for the process?

- AITS
- Auditors
- Business managers
- Representative from each group who owns each application
- USC

Chapter 10: Current State Metrics

Metrics in three areas is being collected on each process. These metrics will be used to measure success in the future state. [Enter the metrics to each question listed below.]

- How long does the process take from start to finish?
 - 1 to 3 days
Current target is to complete the process within 3 business days when complete information is provided within the request.
- How many touchpoints are there per process?
Depending on the type of request the process can have a minimum of five touch points and as many as nine touch points.
- How many steps are involved in each process?
 - Depending on the type of request the process can have a minimum of 13 steps within the process and as many as 31 steps in the process.

Chapter 11: Feedback from Customer Focus Groups – Current State

The Current State process was presented to each University's Customer Focus Group on Tuesday, January 23, 2018 and Wednesday, January 24, 2018. A total of 5 people attended with one person in attendance from UIC, zero people from UIS, and four people from UIUC.

University Focus Group Summary

At each of the University Focus Group meetings, the attendee were presented with the major process steps and a description of the tasks completed within each of the three main identified steps within the process.

The units follow the process described. Issues identified were with the SecApp and the difficulty a USC has in determining what access a user needs to be granted.

University Focus Group Report

Current process

- The Department Units will submit their request to the USC.
- The USC will follow the process as described in the presentation.

Issues

- When the USC determines which access the employee needs to be granted.
- The user felt the process isn't clearly defined on what access a user should receive.
- The USC stated there should be consistency when sending notifications of access granted and denied from all applications.
- Too many systems to set up a user (SecApp, Authority)

Chapter 12: Opportunities for Improvements

The following opportunities for improvement were identified through team discussions, and feedback provided by University focus groups, and from the Director Council. Issues were categorized into six, covering Communications, Documentation, Policy & Procedures, Resources, Technology, and Training. Issues shown in **Bold** are connected to a Recommendation for Improvement in [Chapter 15: Recommendations for Improvements](#)

Communications – Issues related to providing information	
C1	Off-boarding isn't happening as it should
C2	Conflicting actions between Old USC and New USC when an employee changes departments
C3	Employee off-boarding have left active work within the workflow and others don't have access to work
C4	Lack of knowing what access exists
C5	Lack of understanding what access should be requested
C6	Lack of understanding how to request access
C7	Lack of understanding the workflow to process an access request
C8	Understanding the amount of time required to configure access correctly/accurately
C9	Lacks consistency when sending notifications of access granted and denied from all applications
C10	Not knowing what access to request for Banner

Documentation – Issues related to lack of documentation	
D1	Conflicting actions between Old USC and New USC when an employee changes departments
D2	Lack of 'Access Profiles' that specify what access each position should be given
D3	Lack of knowing what access exists
D4	Lack of understanding how to request access
D5	Lack of documentation
D6	Lack of understanding the workflow to process an access request
D7	Not knowing what access to request for Banner
D8	Lack of knowing approved department head

Policy/Procedures – Issues related to Procurement Policies and Procedures

P1	Off-boarding isn't happening as it should
P2	Conflicting actions between Old USC and New USC when an employee changes departments
P3	Lack of 'Access Profiles' that specify what access each position should be given
P4	Employee off-boarding have left active work within the workflow and others don't have access to work
P5	Lack of understanding what access should be requested
P6	Not knowing there are outstanding charged transactions prior to canceling a charge card

Resources (Financial, Human) – Issues related to lack of sufficient staff or funding

R1	Human input error
R2	Lack of documentation
R3	Understanding the amount of time required to configure access correctly/accurately

Technology – Issues related to system's lack of functionality to support the process

T1	Off-boarding isn't happening as it should
T2	Lack of 'Access Profiles' that specify what access each position should be given
T3	Employee off-boarding have left active work within the workflow and others don't have access to work
T4	Manual process to inactivate all access
T5	Human input error
T6	Lack of understanding the workflow to process an access request
T7	Understanding the amount of time required to configure access correctly/accurately
T8	Lacks consistency when sending notifications of access granted and denied from all applications
T9	Not knowing what access to request for Banner

Training – Issues related to lack of understanding the process

TR1	Conflicting actions between Old USC and New USC when an employee changes departments
TR2	Employee off-boarding have left active work within the workflow and others don't have access to work
TR3	Lack of knowing what access exists

24.0 System Security Authority

Training – Issues related to lack of understanding the process	
TR4	Human input error
TR5	Lack of understanding what access should be requested
TR6	Lack of understanding how to request access
TR7	Lack of understanding the workflow to process an access request

Chapter 13: Suggested Improvements

The following recommendations came from discussions with the process team members, and/or the Director Council, and/or University System focus groups. Not all improvements were selected by the process team. The selected improvements were presented to the University focus groups for feedback, and are recommended from review by the Director Council. A Suggested Improvement displayed in **bold** is associated with a Recommendation for Improvement, and is further discussed in [Chapter 15: Recommendations for Improvements](#)

Number	Category	Suggested Improvement
1	Communications	List of available access (profiles) that can be granted
2	Communications	Create a visual workflow to communication timeline to create access, and update when moving to a new system application
3	Documentation	Document process and procedures for on-boarding and off-boarding
4	Documentation	Create basic profiles for positions
5	Documentation	Document process and procedures for who to contact to request access
6	Documentation	List of Department Heads and their chart/org
7	Documentation	Define a purchase officer profile (full access, except for charge card access)
8	Technology	System notification when access has been granted on all applications

Chapter 14: Feedback from Customer Focus Groups – Future State

The Future State process was presented to each University's Customer Focus Group on February 27 & 28, 2018. A total of 6 people attended with 3 people in attendance from UIC, zero people from UIS, and 3 people from UIUC.

Customer Focus Group Summary

At each of the Customer Focus Group meetings the six recommendations for improvement were presented along with the Future System Requirements. Feedback was requested after each presented recommendation. Overall each attendee felt each the six recommendation would be very helpful. On the recommendation regarding Off-boarding, each group discussed the issue related assigning a Proxy in the TEM application, the employee leaves who granted the proxy and there isn't a way to remove the proxy.

Customer Focus Group Report

Recommendation feedback:

Provide a list of available access profiles for the applications Procurement Services and Purchasing provide support to

Each group supported this recommendation.

- Very much in favor, due to the difficulty in determining what access needs to be granted to an employee
- The current problem is where there is a conflict to know the difference between what each profile's access contains
- In favor, currently struggling with know what access to give for a particular screen, and giving to much access which is not needed.

Create a visual workflow to communicate the timeline to create/grant access to the Procurement Services and Purchasing applications.

Each group supported this recommendation.

- This will be very helpful with new employees

Document the process and procedures for on-boarding and update of access to the Procurement Services and Purchasing applications.

Each group supported this recommendation.

- Current response is very timely, access is granted within one business day
- Likes the current process, response is quick

Create a project to capture and document the process and procedures for off-boarding of a Procurement Services and Purchasing applications.

Knowing this is outside the scope of this process, each group supported this recommendation

- Could help address contact information as part of the change order process
- When an employee leaves, that person doesn't always get removed as a proxy
- Unable to unsubscribe a proxy when the employee leaves
- Current department will send an email when an employee leaves notifying to request access

Create two new profiles to be used within the applications that Procurement Services and Purchase support.

Each group supported this recommendation

- It would be nice to copy an employee's access to another or new employee, this would help
- Helpful to the default basic user profile

24.0 System Security Authority

Provide system notifications when access has been granted to the applications Procurement Service and Purchasing provided support to.

Each group supported this recommendation

- Didn't know the system didn't do this
- Would be helpful when notifications are received, both USC and Users receiving the email is great

Other

TEM training is telling us to State "see Header", but they still reject some on which that's done.

Chapter 15: Recommendations for Improvements

The recommendations have been identified for improvement. Three different categories were identified for the improvements, and each improvement received a level of implementation. The categories include Communication, Documentation, and Technology. There are two levels of implementation: “short-term” indicates improvements suggested for the current system and process prior to the development of an RFP, and “long-term” indicates improvement to the process with an RFP for a new system. The recommendations are in order to make the process better, help the users understand the process, and make sure the process works.

Number	Describe Potential Solutions	Category	Implementation Level	Related Issue(s)
1	<p>Provide a list of available access profiles for the applications Procurement Services and Purchasing provide support to</p> <p>We are recommending providing a list of available access profiles for the applications Procurement Services and the Purchasing departments provide support to. This list will be available to the department managers and business managers at each University so they will be able to request accurate access for their new employee or additional access to an existing employee. The employee will be able to receive access quicker and be able to begin using system tools to perform their job duties sooner.</p> <p>Examples of some information to be included in the list would be:</p> <ul style="list-style-type: none"> • Application (Banner, iBuy, iCS, and TEM) • Profile • Class Access (e.g. form, query, maintenance) • Form(s) • Process <p>The working team on this project involve the following:</p> <ul style="list-style-type: none"> • AITS - System Access Management • AITS - ADST SecApp DEV • Purchasing departments from each University • University Payables 	Communications/ Documentation	Short Term	C4, C5, C10, D2, D3, D4, D5, D7, T2, T9, TR3, TR5,

24.0 System Security Authority

Number	Describe Potential Solutions	Category	Implementation Level	Related Issue(s)
2	<p>Create a visual workflow to communicate the timeline to create/grant access to the Procurement Services and Purchasing applications.</p> <p>Create a visual workflow of the steps involved in processing a request access to the Procurement Services and Purchasing applications. The OBFS website is the recommended location to provide the information to University employees.</p> <p>By providing this information to University employees, they will be able to understanding the flow of the work within the process; know who to request access from; and if during the process an issues arises one would know where in the process the issue needs to be resolved at.</p> <p>The working team includes:</p> <ul style="list-style-type: none"> • Department Units • Unit Security Contacts (USC) • University Payables • AITS – ADST SecApp Dev • OBFS – BSS – Communication and Instructional designers 	Communications	Short Term	C2, C5, C6, C7, C8, D1, D4, D5, D6, D7, P2, P5, R2, T6, T7, T9, TR5, TR6, TR7

Number	Describe Potential Solutions	Category	Implementation Level	Related Issue(s)
3	<p>Document the process and procedures for on-boarding and update of access to the Procurement Services and Purchasing applications.</p> <p>The documented process will provide the following:</p> <p>Procedures that need to be completed to obtain access for a new employee or additional access updates for an existing employee.</p> <p>Define who to contact with questions throughout the process.</p> <p>Where to find the list “Find my USC”</p> <p>The documentation will be available to the department managers and business managers at each University.</p> <p>The team hopes to improve the accuracy when submitting an access request, and provide an understanding of what is involved to grant access. The team also hopes the employee will be able to receive access quicker and be able to begin using system tools to perform their job duties sooner.</p>	Documentation	Short Term	C2, C5, C6, C7, C8, D1, D4, D5, D6, D7, P2, P5, R2, T6, T7, T9, TR5, TR6, TR7

24.0 System Security Authority

Number	Describe Potential Solutions	Category	Implementation Level	Related Issue(s)
	<p>The working team on this project involves:</p> <ul style="list-style-type: none"> • AITS - System Access Management • AITS - ADST SecApp DEV • Purchasing departments from each University • University Payables • University Department Units 			
4	<p>Create a project to capture and document the process and procedures for off-boarding of a Procurement Services and Purchasing applications.</p> <p>The documentation will be available to the department managers and business managers at each University. The documented process will provide the procedures that need to be completed when an employee leaves a department who has access to a Procurement Services or Purchasing application.</p> <p>The working team on this project involve the following:</p> <ul style="list-style-type: none"> • AITS - System Access Management • AITS - ADST SecApp DEV • Purchasing departments from each University • University Payables • University Department Units 	Documentation	Short Term	C1, C3, D1, P1, P2, P4, P6, T3, T4, TR1, TR2
5	<p>Create two new profiles to be used within the applications that Procurement Services and Purchase support.</p> <p>We are recommending creating a basic profile for standard functionality for the applications used to access the Procurement Services and the Purchasing departments system functionality. The basic profile will be included in the list of available profiles that is given to the department managers and business managers at each University to use when determining the access to request for their new employee or additional access to an existing employee.</p> <p>The team is also requesting to create a Super User category for the Purchasing office. This will allow them full access to the purchasing applications, but exclude access to Card Services.</p> <p>The working team on this project involve the following:</p> <ul style="list-style-type: none"> • AITS - System Access Management • AITS - ADST SecApp DEV 	Documentation/ Technology	Short Term	C2, C4, C5, D1, D2, D3, D4, P1, P2, P3, P5, T2, TR1, TR3, TR

24.0 System Security Authority

Number	Describe Potential Solutions	Category	Implementation Level	Related Issue(s)
	<ul style="list-style-type: none"> Purchasing departments from each University University Payables 			

Number	Describe Potential Solutions	Category	Implementation Level	Related Issue(s)
6	<p>Provide system notifications when access has been granted to the applications Procurement Service and Purchasing provided support to.</p> <p>Create a project to perform an analysis of the workflow within SecApp to add checkpoints, so at the completion of the entire access request when all parts of the request has been granted an automated email is sent to the USC and the end user notifying the access has been granted.</p> <p>The working team members include:</p> <ul style="list-style-type: none"> • AITS - ADST SecApp DEV • Department Units • Department Unit Security Contacts (USC) • Procurement Services – University Payables • Purchasing departments • OBFS – AVP Business Finance office – University Contract Records office. 	Technology	Short Term	C2, C9, D1, P2, T8, TR1

Chapter 16: Solutions Prioritization Matrix

The recommendation for improvements were reviewed and the potential solutions were prioritized by the Director Council. The below matrix contains the potential solutions for short term implementation and each ranked score.

Solution Prioritization Matrix: System Security & Authority								
	Describe Potential Solutions	Category	Ease of Implementation:	Permanence of the Solution:	Impact of the Solution:	Cost of the Solution:	Total Score (Average of The total product from each participant):	Ranking
			1 (very difficult) - 5 (very easy)	1 (temporary) - 5 (permanent)	1 (low) - 5 (high)	1 (high) - 5 (low)		
			Avg of attribute from each participant)	Avg of attribute from each participant)	Avg of attribute from each participant)	Avg of attribute from each participant)		
1	Provide a list of available access profiles for the applications Procurement Services and Purchasing provide support to	Communications/ Documentation	3.63	3	2.88	3.63	167.5	1
2	Create a visual workflow to communicate the timeline to create/grant access to the Procurement Services and Purchasing applications.	Communications	3.25	2.75	2	2.75	65.25	3
3	Document the process and procedures for on-boarding and update of access to the Procurement Services and Purchasing applications.	Documentation	2.75	2.13	1.88	3	36.5	5
4	Create a project to capture and document the process and procedures for off-boarding of a Procurement Services and Purchasing applications.	Documentation	3	2.5	2.25	2.5	48.25	4
5	Create two new profiles to be used within the applications that Procurement Services and Purchase support.	Documentation/ Technology	1.5	1	1.13	2	3.75	6

24.0 System Security Authority

6	Provide system notifications when access has been granted to the applications Procurement Service and Purchasing provided support to.	Technology	2.75	3.38	3.13	2.38	84.5	2
7								

Chapter 17: Future State SIPOC Diagram

Process Name	Date
24.0 System Security Authority Current State	March 2018

SUPPLIERS	INPUTS	PROCESS	OUTPUTS	CUSTOMERS
<u>Who</u> provides input to the process	<u>What</u> goes into the process	<u>How</u> the inputs are transformed to outputs	<u>What</u> comes out of the process	<u>Who</u> received the outputs of the process
AITS – Enterprise System Coordination - Finance AITS - System Access Management Authorizer Group Sec App* Service Desk Manager* University Department Unit/Employee USC	Approval from data managers Basic User information Request for new/update to access	Identify need for new/update access Grant/reject access request Finalize access	Access to a system application Response to the requestor Denial of access and reason Terminated access	UCRO University Department Unit/Employee USC

*Suppliers may change if a new system is put in place

Chapter 18: Future State Requirements

This is a comprehensive list of functional requirements and technical requirements for the future state of the System Security and Authority process. Excluded from this list are any requirements for functionality outside of the scope of this specific process, such as security, accessibility, etc, which will be handled in a different process.

1. Ability to have automated workflow
2. Ability to have one entry point to request access
3. Ability to have a status assigned to the request
4. Ability to view the status of the request as it moves through the workflow to be processed
5. Ability to define profiles for purchasing and procurement services
6. Ability to define profiles for purchase roles
 - a. The ability to define dollar limit access
 - b. The ability to define dollar limit access at different levels
7. Ability to have levels of approvals
 - a. Director/Department head

Chapter 19: Subject Matter Expert Team

The following individuals participated on the Subject Matter Expert Team of the BPI System Security Authority/Credit Card On-boarding project:

Name	University/Department	Title
Deborah Caparoon	UIUC/Facilities and Services	Bus/Adminv Assoc
Kevin Fair	UIC/Purchasing	Associate Director
Robert Law	University of Illinois System Office/AITS	Data Security Spec
Hilarie Maloney	University of Illinois System Office/AVP Business & Finance	Coord BSFIN
Kandra Miller	University of Illinois System Office/Payables	Asst Dir Univ Payables
Michael Nevill	University of Illinois System Office/AITS	Asst Dir TAM
Sara Simmons	University of Illinois System Office/AVP Business & Finance	Coord Univ Contract Mgmt Syst
Nelly Davis	UIUC/OBFS – AVP Business & Finance	Business/Administrative Associate
Darren Strater	University of Illinois System Office/Payables	Assoc Dir Support Services

Chapter 20: University Focus Group Participants

The following list of individuals participated in a University Focus Group meeting either during the current state and/or the future state of the BPI System Security Authority and Charge Card On-boarding project.

Name	University
Penny Benner	UIUC
Rene Dunnam	UIUC
Angie Helmuth	UIUC
Denise Lee	UIC
June Luna	UIUC
Jessica Salgado	UIC
Mary Urbina	UIC

Appendix A: Business Glossary

USC

Unit Security contact