



—
HOWDY!

DSA IT Liaisons Communications Committee
2/4/2020

► Agenda

- Tech Tip: FileX File Transfer Utility
- Incident Management Process
- Customer Notifications & Communication
- This month in DoIT
- Q&A

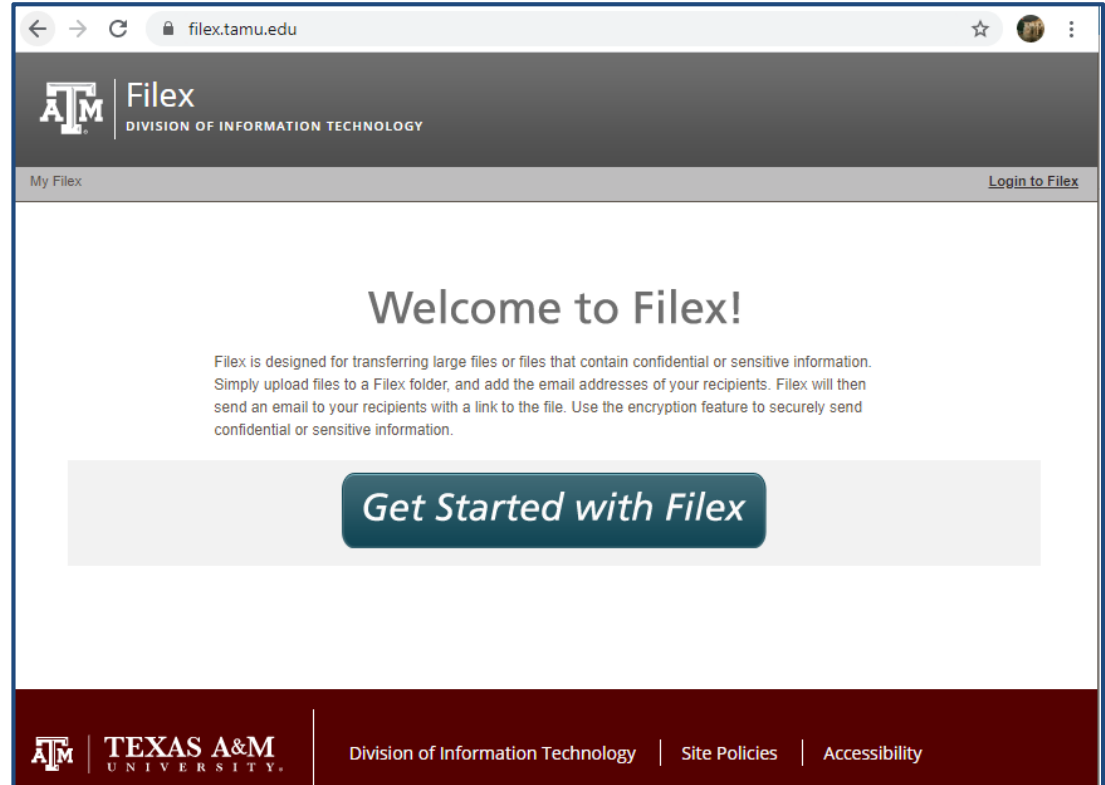
FileX File Transfer Utility

► Tech Tip: FileX File Transfer Utility

- The Filex file distribution system provides a secure way to transfer files, including files too large to send as an email.
- For files containing sensitive or confidential information, Filex includes an encryption option.
- Filex is not a long-term storage solution. Files will remain available on the Filex system for three days. After three days, the files are automatically deleted from the Filex server and cannot be recovered.

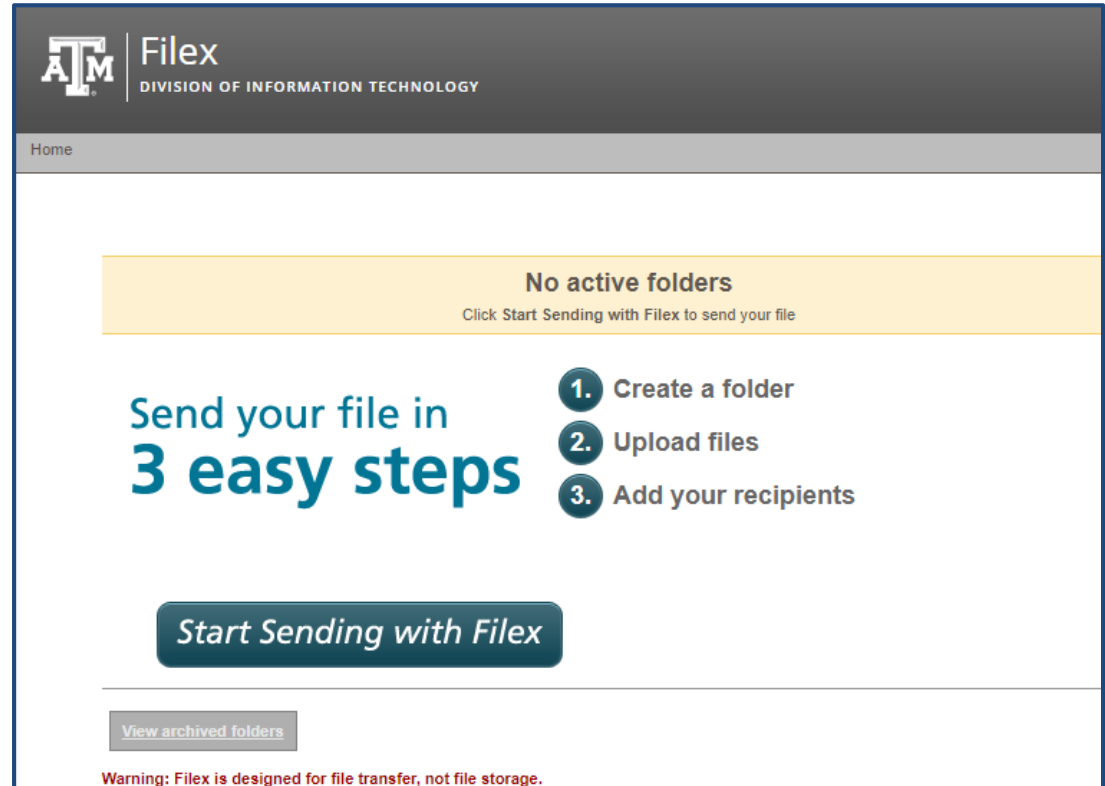
Tech Tip: FileX File Transfer Utility

- Access the utility by visiting filex.tamu.edu
- Login using NetID and password



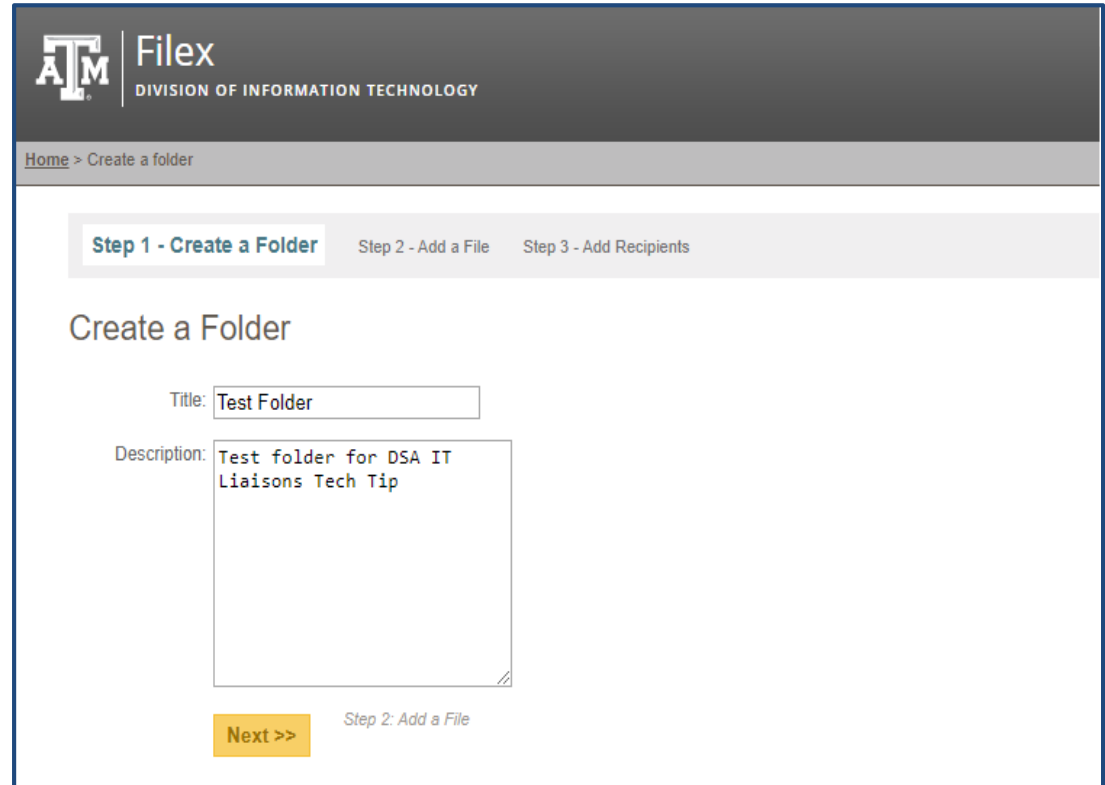
Tech Tip: FileX File Transfer Utility

- Select “Start Sending with Filex”



Tech Tip: FileX File Transfer Utility

- Step 1: Create a folder to store your file(s)



The screenshot displays the FileX File Transfer Utility interface. At the top, the header includes the TAMU logo and the text 'FileX DIVISION OF INFORMATION TECHNOLOGY'. Below the header, a breadcrumb trail shows 'Home > Create a folder'. A progress bar indicates three steps: 'Step 1 - Create a Folder' (active), 'Step 2 - Add a File', and 'Step 3 - Add Recipients'. The main content area is titled 'Create a Folder'. It contains a 'Title:' label with a text input field containing 'Test Folder'. Below this is a 'Description:' label with a text area containing 'Test folder for DSA IT Liaisons Tech Tip'. At the bottom, there is a yellow 'Next >>' button and a link for 'Step 2: Add a File'.

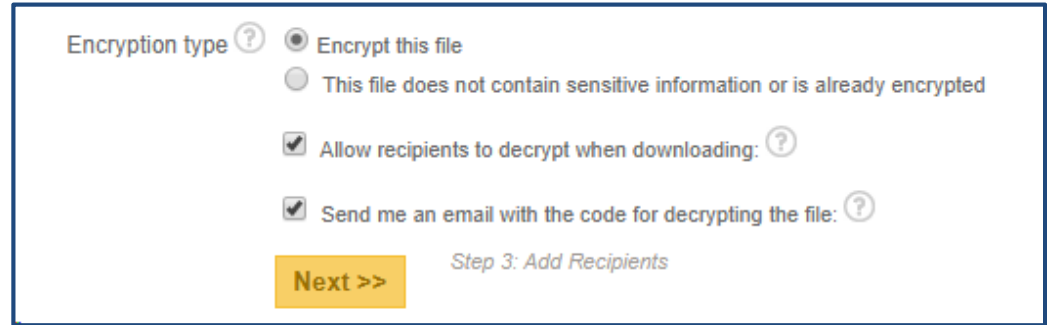
Tech Tip: FileX File Transfer Utility

- Step 2: Provide a name and description for the file and add the file

The screenshot displays the FileX File Transfer Utility interface. At the top, the TAMU logo and 'FileX DIVISION OF INFORMATION TECHNOLOGY' are visible. Below the header, a breadcrumb trail reads 'Home > Test Folder > Add New File'. A progress bar shows three steps: 'Step 1 - Create a Folder', 'Step 2 - Add a File' (which is highlighted), and 'Step 3 - Add Recipients'. The main section is titled 'Add a File' with a 'Skip' button. It contains a 'Title' field with the text 'DSA IT Liaison Presentation' and '(optional)' to its right. Below this is a 'Description' field with a text area containing 'The attached file contains the DSA IT Liaison Presentation from 2/4/2020' and '(optional)' to its right. The 'File' section shows a 'Choose File' button, the filename 'DSA Li... .pptx', and the note 'maximum file size is 2 GB.'. Under 'Encryption type', there are two radio buttons: 'Encrypt this file' (which is selected) and 'This file does not contain sensitive information or is already encrypted'. A 'Next >>' button is at the bottom, and the text 'Step 3: Add Recipients' is visible to its right.

Tech Tip: FileX File Transfer Utility

- For files containing confidential data (i.e. FERPA) select “Encrypt this file”
- You’ll be provided a decryption code the recipient will need to decrypt the file



Encryption type ?

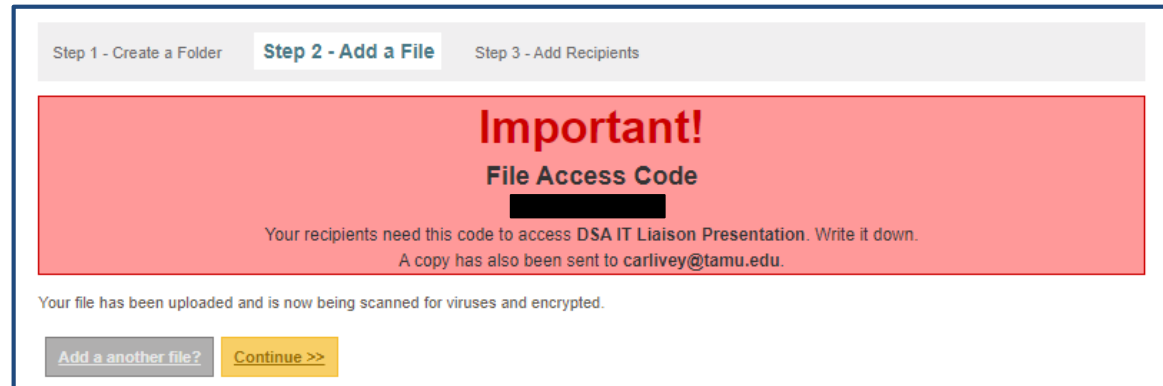
☒ Encrypt this file

☐ This file does not contain sensitive information or is already encrypted

☒ Allow recipients to decrypt when downloading: ?

☒ Send me an email with the code for decrypting the file: ?

[Next >>](#) *Step 3: Add Recipients*



Step 1 - Create a Folder **Step 2 - Add a File** Step 3 - Add Recipients

Important!

File Access Code

[REDACTED]

Your recipients need this code to access DSA IT Liaison Presentation. Write it down.
A copy has also been sent to carlivey@tamu.edu.

Your file has been uploaded and is now being scanned for viruses and encrypted.

[Add a another file?](#) [Continue >>](#)

Tech Tip: FileX File Transfer Utility

- Step 3: Add recipients and grant folder access

The screenshot shows the 'Step 3 - Add Recipients' interface of the FileX utility. At the top, there are three tabs: 'Step 1 - Create a Folder', 'Step 2 - Add a File', and 'Step 3 - Add Recipients', with the third tab being active. Below the tabs, the heading 'Add Recipients' is displayed next to a 'Skip' button. A sub-header states, 'Recipients will have access to all the files in this folder'. The form includes an 'Email:' field with the value 'carlivey@tamu.edu' and a 'Recipient:' dropdown menu currently set to 'can download'. Below these fields is a blue link labeled 'Add Another' and a yellow 'Complete' button. On the right side, a yellow callout box provides instructions: 'In this step, give people access to this folder.' followed by a bulleted list of permission levels: 'Can download only.', 'Can download and upload.', and 'Has complete access.'. A final note in the box states: 'Recipients with complete access can delete files, edit folder titles and descriptions, and add or remove recipients in addition to uploading and downloading.'

Step 1 - Create a Folder Step 2 - Add a File **Step 3 - Add Recipients**

Add Recipients

Recipients will have access to all the files in this folder

Email:

Recipient:

[Add Another](#)

[Complete](#)

In this step, give people access to this folder.

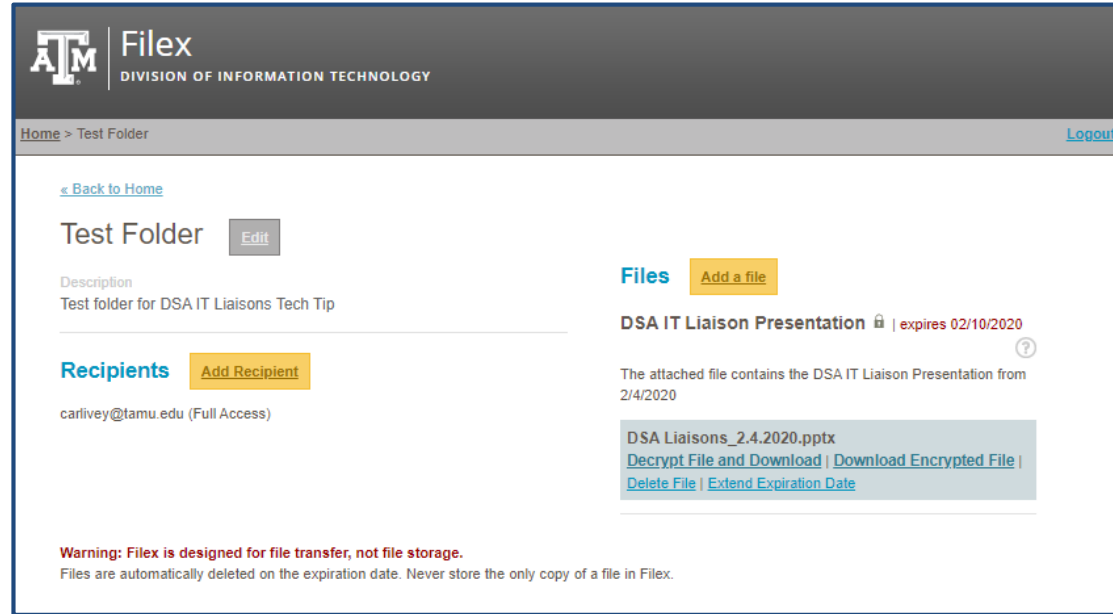
- Set permission levels for each recipient:
 - Can download only.
 - Can download and upload.
 - Has complete access.

Recipients with complete access can delete files, edit folder titles and descriptions, and add or remove recipients in addition to uploading and downloading.

Tech Tip: FileX File Transfer Utility

Notes:

- Always encrypt files containing confidential information!
- Send recipients the decryption key when encrypting files!



For more info visit [Protecting Confidential Information](#)

Incident Management Process

Carl Ivey

► Incident Management Process

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations.

Incident

An unplanned interruption to an IT Service or reduction in the Quality of an IT Service. Failure of any Item, software or hardware, used in the support of a system that has not yet affected service is also an Incident.

Help Request *(not in scope of the Incident Management Process)*

A request from a user that initiates a service action which has been agreed as a normal part of service delivery (i.e. access requests, reports, licensing, questions)

► Incident Management Process

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations.

This sometimes means providing the user with a suitable workaround to get them back up and running if a permanent fix would cause further delays.

Example: A multifunction printer used by an entire office is not working properly. Users are provided access to a nearby printer to enable them to print until the multifunction printer is fixed.

Incident Management Process

- DoIT Staff work with customers to understand the Urgency and Impact of the incident

Urgency + Impact = Priority

Incident Priority			Impact			
			1 - Critical - All Customers / Entire Campus	2 - Serious - Department / Building	3 - Moderate - Group / Floor	4 - Minimal - Individual / Office
			Multiple departments are affected. Public facing service is unavailable.	All customers in one department are affected.	One group or sub-group in one physical location is affected.	One customer is affected.
Urgency	1 - High	Service or major portion of a service is unavailable.	1 - Critical	2 - High	2 - High	4 - Normal
	2 - Medium	Issue prevents the user from performing critical time sensitive functions.	2 - High	3 - Medium	3 - Medium	4 - Normal
	3 - Low	Issue prevents the user from performing a portion of their duties.	3 - Medium	3 - Medium	4 - Normal	4 - Normal
	4 - Minimal	Issue it not currently affecting any users or affect has no time sensitivity.	3 - Medium	4 - Normal	4 - Normal	5 - Planning

Incident Management Process

- DoIT Staff work with on Incidents according to Priority

		≡ Number	≡ Record type	≡ Classification	≡ State	≡ Caller	≡ Short Description	≡ Service	≡ Opened	≡ Priority ▲	≡ Assignment group	≡ Assigned to
		INC-20200908	Incident	Help Request	Open	Jaidi Muehle	MSU L&L results please instant interface services	Print and Click (TAMU-DSA)	2020-09-08 09:04	2 - High	Systems (TAMU-DSA)	Michael Joubert
		INC-20200909	Incident	Incident	In Progress	Scott Joubert	Spout Choke Unresponsive ACM Termination Issue	Res. Desk (TAMU-DSA)	2020-09-09 07:58	3 - Moderate	Resolutions (TAMU-DSA)	Deanna Moline
		INC-20200912	Incident	Network Network Status - Incident	On Hold	Edie Barker	Virtual Network Folder Access	Edie Barker (TAMU-DSA)	2020-09-07 09:00	4 - Low	Service Desk Level 2 (TAMU-DSA)	Samuel
		INC-20200912	Incident	Office Desktop Software	On Hold	Edie Barker	group policy preventing printing report to pdf	Workstation Software (TAMU-DSA)	2020-09-07 02:00	4 - Low	Service Desk Level 2 (TAMU-DSA)	Deanna Moline
		INC-20200912	Incident	Google Chrome	On Hold	Edie Barker	Google Chrome Save As	Workstation Software (TAMU-DSA)	2020-09-07 02:00	4 - Low	Service Desk Level 2 (TAMU-DSA)	Samuel
		INC-20200912	Incident	Google Chrome	On Hold	Edie Barker	Google Chrome Save As	Workstation Software (TAMU-DSA)	2020-09-07 02:00	4 - Low	Service Desk Level 2 (TAMU-DSA)	Samuel

- If Level 1 Service Desk Technicians are unable to resolve the Incident or provide an adequate workaround, the Incident is assigned to an appropriate Provider Group (Team) within DoIT.

► Incident Management Process

Incident States

- **New** – has not been worked on
- **In Progress** – actively being worked on
- **On Hold**
 - Awaiting Caller, Awaiting Change, Awaiting Problem,
 - Awaiting Vendor, Awaiting Decision
- **Queued** – customer has responded and/or needs to be worked on
- **Scheduled** – work has been scheduled for a future time
- **Resolved** – ticket has been Resolved
- **Closed** – ticket closed 7 days after Resolved

► Incident Management Process

Best Practices

- **New** - Provider Groups (DoIT Teams) seek to communicate with Customers within 1-2 days of receiving Incidents
- **On Hold, Awaiting Customer** - Customers respond to requests from Level 1 technicians and Provider Groups within 1-2 days
- **Queued** - Provider Groups review customer responses within 1-2 days
- **Scheduled** - Provider Groups will attempt to schedule work and annotate Incident work notes for Liaison awareness and communication

Customer Notification & Communication

Justin Ellison

► Customer Notification & Communication

- What communications do you expect from DoIT?
 - DoIT Outages and Upgrades affecting Service Levels?
 - DoIT Upgrades and Maintenance not affecting Service Levels?
- How do you want to receive communications?
 - DSA All User Emails?
 - Liaison one-on-one
- What communications do you find helpful when meeting with your Liaison?

► Customer Notification & Communication

- Scenario 1
 - An emergency security patch for a database server is released by a vendor. Before noon, DoIT admins install the patch on a test system and observe no downtime and no apparent issues. DoIT admins decide that due to the severity, the patch will be installed into the production database servers at 6pm. Although the complexity is greater with the production system, admins expect no downtime for the 15 vendor applications utilizing the database server.
- Questions
 - Should DoIT notify Division customers?
 - Whom should DoIT notify?

► Customer Notification & Communication

- Scenario 2
 - At 8:30am, DoIT identifies an unresponsive server using the server monitoring system. By 8:45am the server is back online and the applications A, B, & C it was hosting are available. It was determined that the applications were likely unavailable for 4 hours. DoIT responded to 3 customers that contacted the service desk informing them that application A is once again is available. However, DoIT received no reports about applications B & C.
- Questions
 - How should DoIT notify Division customers?
 - Whom should DoIT notify? (Scope)

This month in DoIT

Carl Ivey

► This month in DoIT

- **Successfully Completed CAPS Consolidation**
- **CAPS PNC Implementation nearing completion**
- **DOJ Accessibility Audit underway**
- **Interviews underway: SAD II/PM II on-site, SysAdm Phone**
- **DoIT CPR on hold**
- **Annual Information Security Risk Assessment coming soon**
- **TAMU Technology Summit in Galveston, TX Feb 16-18**
- **Laserfiche Conference in Long Beach, CA Feb 11-14**

Department Q&A

Carl Ivey