Minutes for Delaware Continuity Coordinator Council

November 17, 2017
1 p.m. – 3 p.m.

Attendees: Sandra Alexander, Dan Cahall, Thomas Cuccia, Jennifer Dittman, William "Paul" Dunworth, Mike Erixson, Patricia Gannon, Lori Gorman, John Healy, Adrienne Hegman, Erich Heintz, Lynn Hooper, Alyssa Huenke, Brian Leahy, Tony Lee, Tim Li, Kathleen Mahoney, John Mancus, Anthony Manson, Claudette Martin-Wus, John McCartney, Bill Miller, Faith Mwaura, Linda Popels, Choxi Punita, Chris Ramos, Gary Rauso, Michelle Strauss, Syd Swann, Doyle Tiller, Terri Timmons, Karen Trimmer, Amy Woodward, Kevin Wright,

- **DECCC Updates**
  - Elections held for Council Members
    - Positions Filled:
      - Vice-chair- Linda Popels
      - IT Systems Officer- Dan Cahall
      - Education and Training Officer- Patricia Gannon
      - Vital Records Officer- open
    -
  - Upcoming Training Opportunities:
    - Crisis Communication Refresher Training-
      - Dec. 6th 9-11 AM, Kent County
      - Dec. 13th 1-3 PM, New Castle County
    - ICS-300 Intermediate- Jan 9th-11th 8:30-4:30 http://www.dema.delaware.gov/services/calendar/Trng_Cal.shtml
  - NSA Day of Cyber School Challenge
    - Available to students grade 9-12, higher education, adult learners
    - Statewide program that allows you to experience a day in the life of the nation's top cybersecurity experts- in just three hours
    - Participate in challenging real-life cyber scenarios, discover the skills and tools used by the NSA, and explore the vast number of careers in cybersecurity
  - HR/Employee Update Process- getting report with Contact information from PHRST
    - Contact HR to see if they have access to run "PHRST End User Query"
    - Send Email to employees requesting they update contact data in self-service portal- suggested email template on DECCC site.
    - Request HR to run query
    - Send file to DTI BCDR liaison for format correction and import into BCIC.
    - Run Crisis Communication test and contact employees with inaccurate information.

- **More BCIC updates/ training- PPT attached**

Lori Gorman, Dept. of Technology and Information

- Application Updates- flagging, colored views
- Using To-DO's
- Employee Update Process- refresher

- **DOL Cyber Breach- PPT attached**
  Erich Heintz, Dept. of Labor
  Dept. of Labor Unemployment Insurance shares their experiences with a Cyber Breach and some of their Lessons Learned.

- **Disaster Recovery- Fire and Water Damage Remediation Services Contract**
  Doyle Tiller, Dept. Facilities Management
  Listen to break down of the Fire and Water Damage Remediation Service contract recently awarded to learn about potential vendors that should be included in your COOP plans to handle facility related damage restoration.

- **Q & A**
  - **Q:** *Is the NSA Day of Cyber Challenge available to 8th graders?*
    A: No- available participants must be in the 9th grade or older.

  - **Q:** *What codes apply regarding the re-occupancy of a building after an incident?*
    A: Building occupancy is determined by multiple factors including the type and location of the incident (i.e.- fire in the wall vs. an open location), and the responding parties. This may include city, state, and municipality codes and will involve multiple organizations such as Fire, polices, building owners, insurance, etc.

  - **Q:** *Earthquake discussion*
    A: https://www.shakeout.org/southeast/delaware/

DECCC Steering Committee members:

Tony Lee – Co-Chair
Lori Gorman – Co-Chair
John Mancus – Disaster Preparedness Officer
Mark Devore– Facilities Officer

Vacant- Vice-Chair
Vacant- Education and Training Officer
Vacant- IT Systems Officer
Vacant- Vital Records Officer

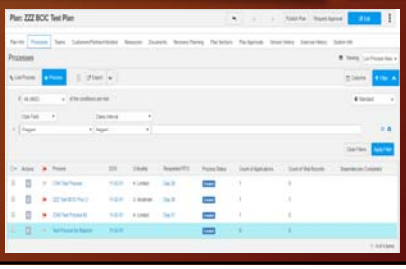
If interested in any of the vacant positions, please contact Lori Gorman

BCIC Updates

Lori Gorman
Sr. Disaster Recovery Specialist
Dept. of Technology and Information

Tool Updates: Flagging

Flagging- added ability to flag records within your plan. This can be used to indicate needed follow-up and to filter by flagged items. Suggest using this option to sort process records for review with specific team leads. Flagging is user specific.

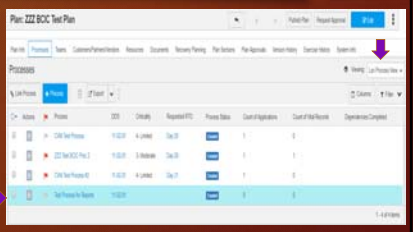


BCIC: Tips & Tricks

- When looking for processes or other data in the plan output- you can do a search on the PDF.
- Use flag & filter to isolate materials when meeting with Team Leads and to indicate a record for follow-up.
- Change your view to see highlighted records (colored view) that are missing data.
- When reviewing Employee Dictionary- use the Employees with DDS Not Assigned to Plan Position/ Process Position to identify employees with your DDS that are not assigned to a team position (linked to your plan).
- Use To-Do's to set automated reminders and deadlines for plan updates.

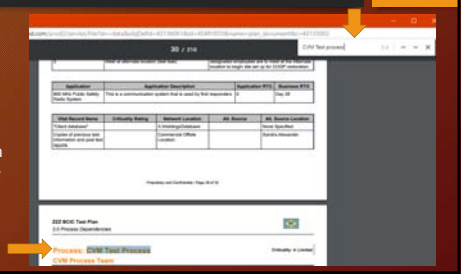
Tool Updates: Color Coded Views

- Color Views- color codes can be added to select views to indicate missing or incomplete data. Examples: Process records missing RTO, Plan vendors missing vendor reps, etc. Custom Color views can be created for specific users by contacting your BCDR Liaison.

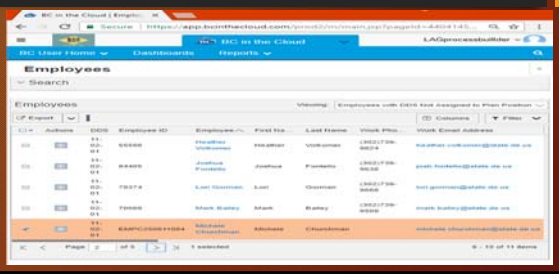


Searching a PDF

- In the plan output, processes are organized by criticality rather than alphabetically. To quickly locate a process (or any other data) in your PDF output, hit CTRL F to open a Find option. This will allow you to quickly search your plan for specific data.



Example Color Views: Employees not assigned to positions



Existing Color Views

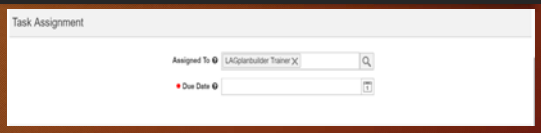
- Process View_ Colored: higlights process records missing Requested RTO (blue).
- Plan Customer is State Entity_colored: highlights customer (business entity) records that with no Main Number (green) or State Employee (yellow) assigned.
- Plan Customer is not State Entity_colored: highlights customer records with no Customer Rep assigned (green).
- Plan Vendors_Colored: highlights Vendor records with no Vendor Rep assigned (green).
- Employees with DDS not assigned to Process Position: highlights employee records with matching DDS that are not assigned to any process team positions (orange)
- Employees with DDS Not Assigned to Plan Position: highlights employee records that with matching DDS that are not assigned to any plan team positions (orange)

Complete To-Do Details

To-Do's

- The BC in the Cloud To-Do function offers COOP Coordinators the ability to create reminders and tasks directly in the tool to assist in Plan maintenance. These To-Do's can be created by any plan builder and assigned to themselves or other COOP Coordinators with matching security (DDS) within their plans. They can be linked to specific plans or processes.

Complete Task Assignment Selection

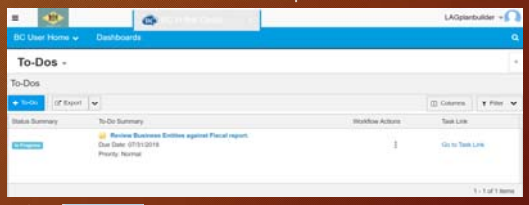


Complete the assigned to field. Assignments must be made to users whose DDS matches that of the To-Do.

Complete the Due Date Field. Reminder Emails will be triggered based on this date. Email reminders will be sent 30 days prior to the due date, to be repeated every 2 weeks. Leading up to that date.

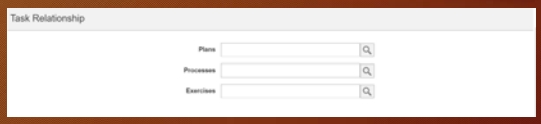
Creating a To-Do

- BC User Home- select To-Do from the drop down.



- Select 

Assign Task Relationships



You may link the tasks to a specific plan, process, or exercise. If no plan, process or exercise is linked to the To-Do, the To-Do will still be created but the task link will not function appropriately.

Update To-Do: Workflow Status

If you completed the task, you may change the status to complete. If this is a task that will need to be repeated, you may wish to only change the due date so that the email reminders will be re-triggered next year.

Employee Update Refresher

- Steps:
  - Go to Employees under the BC User Home dropdown.
  - Search for the Employee name to be added/updated/deleted.
  - Click on the employee name to open the employee record.
  - Review/Update contact information.
  - Click on the Relationships tab to confirm team and call tree assignments.
  - Make any necessary changes.
  - Click Save.

Suggested uses for To-Do's

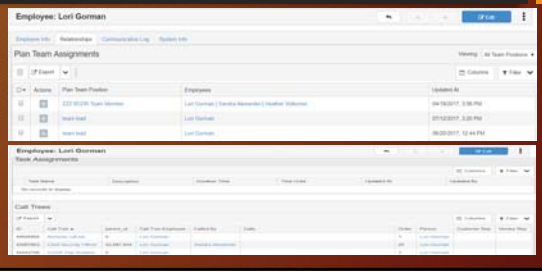
Existing workflows-

- The system will already send you reminders 45, 15, 0 days before your plan is scheduled to expire.
- The system will already send you reminders when an MOU is scheduled to expire.

Suggested uses:

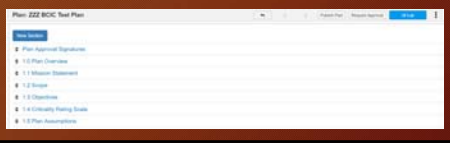
- Set process to-do if you need to return back to a specific process.
- Create To-Do's to break-up the plan update process into manageable sections, or share responsibilities across plan builders
- Create a To-Do related to specific tasks such as annual/ semi-annual, or quarterly Crisis Communciation Tests. Description may include HR contact updates, team updates, call tree updates, Crisis Communication User Group updates.
- Create To-Do(s) related to your annual COOP Drill.

Employee Relationships Tab



Tool Updates: Coming Soon

- In progress: Plan Output-
  - Currently Customers and Vendors related to each process team displays in the process details section (3.0). We are working to have this suppress if blank.
  - Currently updating Plan Sections to allow easier editing of plan specific language.



New Employees

- Finding an employee in the Employee dictionary allows you to update their contact information. THIS DOES NOT LINK THEM TO YOUR PLAN!
- You will need to add any new employees to a team in order to link them your plan.
  - Open your plan or select Teams from the BC User Home Tab.
  - Locate the Process Team or Plan Team you wish to add them too. Select the Plan/Process Team Position to edit the members with your new employee. Remember Process Teams are shared so updating it on one process will update the team through-out your plan.
  - In your plan, go to Call Trees under the Recovery Planning tab to add new employees to any call trees.
  - Select the Edit Action next to your desired Call tree to add their name. SAVE your changes
  - Then Select the Call Tree name to change their location in the Tree. SAVE UPDATES.

Deleted Employees

- Twice a month, a comparison is run against PHRST to compare state employees with the Employee dictionary in BCIC. If an employee has LEFT the state, you will receive an email from your BCDR liaison with the names and warning that they will be removed from the system on a specified date.
- IF they should not be removed, email your BCDR liaison immediately.
- IF they are no longer with your agency, you will need to update your BCIC plan accordingly.
  - Locate the Employee record (Employees under BC User Home tab).
  - Go to the Relationships tab.
  - Select the edit action next to any team assignments and remove the employee. SAVE.
  - Open the Call Tree by clicking on the name.
  - Select the employee name by placing a check in the box. Click on the Trash Icon, Confirm, and Save Updates.
- If you do not remove the employee from all teams and call trees prior to the deletion, it will result in gaps in your plan.

Employee Updates- Crisis Communication

- Once contact data has been added to the employee profile, their information should transfer during the nightly update process.
- The following business day, log in to MIR3 and review your *USER GROUPS* to ensure all new/current employees are present.
- Remember your Organization wide group is dynamic and any new employees with your matching DDS should automatically be added to this group. However if any new employees do not have your DDS (consolidated, payed from other revenue streams, etc.), they will not automatically be added to the dynamic group. You will need to contact your BCDR liaison to have them added to this call tree.
- Any User Groups you wish to include an employee in will need to be manually updated. Example: leadership call groups, after hours call groups, location specific call groups.

Confirming User Groups

Steps:

- Log into MIR3 tool.
- Select the User Tab from the primary bar (top of screen).
- Select Show All under the Groups tab in the secondary bar (left side of screen).
- Open the User Group by clicking on the name.
- Review Checked users- uncheck any users that should not be included.
- Select All to view additional users that are available to add to your group.
- SAVE YOUR CHANGES.

You may also export the list of users to an Excel file for an easier comparison. Check the box next to the user group name and select the EXPORT button located on the bottom right hand side of your screen.

It's the End of the World as We Know It (And I Feel Fine)

Erich Heintz - Department of Labor

Day 2 – 5 (March 16-19)

- Daily calls through the weekend.
- No "new news".

Day 6 (Monday, March 20)

- Very early media coverage has begun based on information leaking from the daily status calls.

Day 7 (Tuesday, March 21)

- Slightly more press coverage.
- Daily call with AJLA-TS is not as "smooth"
- Decision is made to begin more formal interactions beginning the following day.

Who?

America's Job Link Alliance (AJLA) is an alliance of workforce organizations partnering to produce high-quality information technology products to empower workforce agencies to deliver exceptional customer service and drive the economy by connecting employers and job seekers.

America's Job Link Alliance–Technical Support (AJLA–TS) serves as the national information systems development and support center for AJLA.

The DEDOL is a long-time member of the AJLA, along with 15 other U.S. States.

Day 8 (Wednesday, March 22)

- State of DE Cyber Security Incident Response Team stands up.
- DOL begins preparing a statement of what is known
  - Incident has occurred
  - Three states in the consortium impacted
  - Root cause identified and no longer a threat.
  - No evidence that Delaware data has been compromised.

Day 1 (Wednesday, March 15)

On March 15, 2017 the DEDOL was advised that an AJLA-TS managed application suffered a security breach that impacted three of its partner States.

JobLink / ServiceLink / FiscalLink

```
Possible security incident came up in the
past couple of hours, details in report.
I'll advise immediately if it turns into
something real.

Thanks,
Erich
```

Day 8, 12:45PM

- Short notice call for all States
- RSA investigation reveals reconnaissance and attacks took place over the course of weeks
- AJLA-TS is preparing lists of impacted jobseekers and will deliver shortly
- All 10 States have been impacted
- All 10 States have met the criteria for substitute notice

What is Substitute Notice?

If the cost of providing notice will exceed $75,000, or affected Delaware residents exceeds 100,000 residents

1. E-mail notice if e-mail addresses are available
2. Conspicuous posting of the notice on web site
3. Notice to major statewide media.

The DOL fulfilled obligations 2 & 3 by 6:00PM that evening

Lessons Learned

- Excessive records retention
- Misguided or antiquated design decisions
- Rebuilding history

The Result?

After a week of investigation it was revealed that ten States were impacted in the breach, including Delaware. This breach exposed the Personally Identifiable Information of 4.8 million persons nationwide, including up to 250,000 Delaware citizens.

This is the largest breach in State of Delaware history.

Tips for Agencies
Who to call

- Deputy Attorney General
- Security Operations Center
- Insurance Coverage Office;
  - The State of Delaware has breach insurance
- Partner agencies and other stakeholders
- Regulatory boards and commissions
- State legislators

The Response

- Evaluate the system for suitability to return to business.
- Guidance for DOL staff when engaged by citizens
- Substitute notice continuation; Email notification
- Call center setup for inquiries and to assist with credit monitoring
- Ongoing press notifications
- Application changes to mitigate future threats
- Beyond substitute notice; USPS mail notification to citizens who either had no email address on file or whose email bounced back

Tips for Agencies
What to do

- Determine the members of your incident response team early.
- Gather every piece of information you have on the impacted system, technical and business process related
- Provide agency staff with accurate information in sufficient quantity to engage. Don't just discuss, issue written talking points and guidelines.
- Establish a single point of contact for the "hard questions"

State of Delaware

1

DISASTER RECOVERY PLANNING AND PROCEDURES

Agenda

2

1. Background
2. State contract for Services
3. Procedures to follow
4. Water Damage
5. Fire Damage
6. Other Things to consider
7. Questions

Background

3

- Disasters can occur at anytime
- State facilities space- need to protect our employees and customers while continuing to provide services to the public *(essence of COOP)*
- *COOP Coordinators will likely be tasked in a disaster scenario to provide guidance and advice to agency leadership.*
- *Provide you the tools needed to mitigate the damage, respond and restore services.*

State Contract

4

- GSS17775-DSTR_RCVRY
- Work up to $45K, over that contact GSS (Public work bids?)
- Services:
  - Water Extraction
  - Fire, Smoke and Water Damage Restoration
  - Debris Removal
  - Sewage Backup/Overflow
  - Mold Remediation
- Six vendors to choose from

Procedures to Follow

5

- Safety first- is the building safe to occupy?
  - Get expert advice, local building code official
- Protect State equipment and assets, security issues
- Contact Disaster Recovery contractor (24 hours response)
- Contact Insurance Coverage Office (State HR) 302-739-3651
- Initiate COOP plan if needed
- Obtain assistance/resources if needed (Capitol Police, DelDOT, DEMA, DFM, GSS, Public Health, etc.)
- Approve contractor quotation for work (NTE price)
- Formulate plan to oversee contractor work

Water Damage

6

- Stop source of water immediately if possible
- Get the water out ASAP (ideally within 72 hours)
- Water type, different procedures
  - Clean, Gray, Black
- Contact County Public Works (for black water)
- Methods to remove
  - Water extraction
  - Evaporation- air moving equipment
  - Dehumidification-
  - Temperature control (greater risk in summer than winter)
- Inspection- Floor and structure evaluation
- Continuous monitoring

Fire Damage

7

- Usually includes water damage from fire fighting
- Smoke removal (soft materials absorb odor)
- Damage level (light to severe)
- Structural issues due to damage to the building?
- HVAC damage
- IAQ testing after cleanup

Other Things to Consider

8

- Special items (artwork, historical documents, etc.)
- State government records (privacy, security)
- Counselling for persons involved (HR)
- Relocation (COOP or other plan)
- Long term solution, Capital repairs
- IAQ testing, decision to reoccupy
- Other services? May need an emergency declaration from **Agency Head**.
  (Title 29, Chapter 69, § 6907)

9

Questions?

Thank You

10

Doyle Tiller
Indoor Air Quality PM
OMB/Facilities Mngmt
Office 302-739-5644
Cell 302-632-8111
doyle.tiller@state.de.us

Mark DeVore
Chief of Engineering
OMB/Facilties Mngmt
Office 302-739-5644
Cell 302-242-8581
mark.devore@state.de.us