Departmental Contract Administrator (DCA) Training

Contracts and Procurement (CnP)
November 29, 2023
Welcome and Agenda Review
• Contracts and Procurement by the Numbers
• Purchase Orders Tips
• Software Purchasing Guidelines
• Risk Assessment Review and ISOTRAQ
• How to Avoid a Non-Compliance
• DCA Best Practices
• CCARS
• Q&A
CNP by the Numbers

- Number of requests completed last year – 667
- A total of 552 purchase orders were processed and 99 were for over 15K
- 26 new contracts resulted from 17 procurements
- Academic, Health, University Lands, ORM and HR were the top requestors
- A total of 2 FTE’s support contract requests and 1.4 FTE’s support solicitations from the CnP Team

On average, last fiscal year, there was 55 requests in our queue when we received your request. On the highest week, we had 103 requests in our queue.
Required documents were not attached.
For example, the quote(s) is missing or expired (more than 30 days), the GPO reference was not valid, it’s over 100K and an HSP plan is needed.

Extra Steps.
When a purchase order is over $250K, CnP has to take it out of the system and have the EVC approve it via docusign. Vendor is making us sign an order form and it has Privacy or Risk elements.

Helpful.
Use the notes/comments to support the purchase for example if you are waiting for a specific approval or document.

Purchases Over $15K.
You will need to include 3 quotes (informal bid process) from different vendors, unless it is a GPO or using an EAJ to justify purchase. Only interact with PO’s under $15K if there is a change order.

Software Purchase.
All software purchases must be approved by IT Purchasing and have an ISOTRAQ (vendor assessment) review.

Patrick Condra is Your PO Contact.
Software Purchases

- Most software can be bought via DIR or a GPO, so utilize your GPO resources for purchasing software.
- Regardless of the dollar amount, when a department wants to purchase a software, they must go through the following reviews.
Risk Assessment Approach

Information Security Office
Agenda

- When are security risk assessments required?
- What is the process for System Administration only contracts?
- What is the process for Systemwide or Master Service Agreements?
When are security risk assessments required?

• Generally for any technology-based provider or partner, particularly if:
  – The vendor accesses, transmits, stores, or processes any UT data
  – The vendor accesses UT systems or networks
  – UT staff, students, faculty, or UT Select Plan members access the vendors’ systems or networks when UT-owned data is present

• The nature of the data and the amount of integration between the vendor and UT infrastructure determine the level of assessment that is required.

• Security’s role is to advise the business owner of the risk. The business owner (aka Data Owner) has the final decision.
System Administration-only assessments

- Annual volume: 165
- Business staff enter info to ISOTRAQ as early in the process as possible, minimally 2 weeks lead time.
- ISOTRAQ questionnaire includes ? for TX-RAMP
- ISO may meet with business owner and/or vendor to understand the scope of the product or service more completely; assessment request may be modified as a result
Systemwide or MSA assessments

- A “Risk Snapshot” is performed by ISO – very minimal
- Technology products or services require integration into an institution’s infrastructure (networks, etc.) and infrastructure is not homogenous across institutions. **UTS ISO has no visibility into institution’s security.**
- Institutions have different risk appetites: health institutions tend to be more conservative than academics
- Institutions vary in their TX-RAMP determination
- Short story: Institutions must do their own assessments.
Compliance requirements for conducting risk assessments

- **UTS 165 Standard 10: Risk Management**
- **UTS 165 Standard 22: Vendor and Third-Party Controls and Compliance**
- **TAC 202 – Security Controls (DIR Security Controls Catalog)**
- Several other regulatory bodies require periodic and supply chain risk assessments (vendors). Example: HIPAA law
New ISOTRAQ Release (Fall 2023)

Jose Granados, Information Security Analyst
Information Security Office

October 2023
Background

- ISOTRAQ is our existing tool for conducting Third-Party security risk assessments.
- To determine TX-RAMP applicability, we use a separate form called the PSQ (Privacy and Security Questionnaire).
Background

• To simplify and streamline these two processes, we are integrating the PSQ into ISOTRAQ.
Why is this happening?

- Both forms collect/capture similar amounts of information, so there’s an overlap
- Less forms to fill out
- Less waiting

Looks familiar?
Demo

- Let’s take a look at the new version.
Questions?

• We are here to help you navigate through this new process.
• Email secadmin@utsystem.edu for any questions, comments, or any feedback.
How to Avoid a Non-Compliance Purchase

How to avoid non-compliance?

• If you have a purchase order in place and it needs to be changed, contact Patrick Condra before the service begins, so he can edit the PO and this must be done prior to the work or service starting.

• If you used an EAJ and the amount is now over the approved estimated amount, the EAJ has to be updated before any work is started or any payment is made to the vendor with new approvals from your department head.

• In general, any purchase over $1,000 needs a purchase order or a contract in place.

Plan early and execute the purchase in a timely manner.
• **Tip 1: Buy-in** - Work with those in your department to loop you in as they are thinking of procuring services so you can advise on next steps.

• **Tip 2: Checklists** - Use the contracting processing checklist in some form (now found on the CNP website and in CCARS) as you look ahead to the next 4-6 months.
Tip 3: – Monitor/Tracking Tool

Use a contract tracking tool to monitor terms, requirements, and spend.
Tip 3 - Tracking Tool

Use a contract tracking tool to monitor
### Tip 3 - Tracking Tool

Use a contract tracking tool to monitor

<table>
<thead>
<tr>
<th>Invoice #</th>
<th>Invoice Date</th>
<th>Invoice Total</th>
<th>Total Remaining on Contract</th>
</tr>
</thead>
<tbody>
<tr>
<td>13760</td>
<td>12/19/2022</td>
<td>$106,785.00</td>
<td>$427,140.00</td>
</tr>
<tr>
<td></td>
<td>Need HUB Forms with invoice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>$427,140.00</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>$427,140.00</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>$427,140.00</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>$427,140.00</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>$427,140.00</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>$427,140.00</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>$427,140.00</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>$427,140.00</td>
<td></td>
</tr>
</tbody>
</table>

Total: $106,785.00 $427,140.00
DCA Feedback and CCARS Training

• How to search?

1. A huge plus would be if we could view agreements between departments like we used to in the old system. I found it very helpful!
2. The ability to search for uploaded agreements by date.
3. Being able to search for the agreements within your department, regardless of who uploads the agreement.
4. Visibility into my team’s contracts.

• How to run reports?

1. Are we able to run reports on our previous and existing agreements?
Main Takeaways

- CnP’s volume is substantial (667 last year)
- Software purchases MUST go by IT
- Purchase Orders contact is Patrick Condra
- ISOTRAQ has been updated and now includes the PSQ review
- Plan early
- Avoid Non-Compliance
- Leverage Best Practices
- CCARS - Continue Feedback Loop
Future State

• Enhanced CnP website
• Annual Information Sessions
• FAQ’s
• Resource Guide updated
• Terms and Definitions
• Continuous feedback loop
Thank You!
Any questions?